ANNALS OF FACULTY ENGINEERING HUNEDOARA
– INTERNATIONAL JOURNAL OF ENGINEERING
Tome X (Year 2012) – FASCICULE 1 (ISSN 1584 – 2665)

[1.] Ladislav HURAJ, [2.] Vladimír SILÁDI

VOMS CERTIFICATE-BASED AUTHORIZATION IN AD HOC GRIDS

1. DEPARTMENT OF APPLIED INFORMATICS, UNIVERSITY OF SS. CYRIL AND METHODIUS IN TRNAVA, NÁM.J.HERDU 2, TRNAVA, SLOVAKIA
2. DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF MATEJ BEL, TAJOVSKÉHO 40, BANSKÁ BYSTRICA, SLOVAKIA

ABSTRACT: *Trust in grid computing plays a significant role. Traditional grids use various methods for this, mostly centrally oriented ones, such as certification authorities, VO management servers or credentials pools. Ad hoc grids are characterized by absence of a central trust authority; therefore collaborating entities must establish and maintain a trust relationship among themselves. The paper presents a short overview of ad hoc grids and authorization mechanisms. We design a supported authorization mechanism for easier formation of virtual organizations based on VOMS certificates. The mechanism can facilitate the establishment of a trust relationship in cases when standard solutions have failed.*
KEYWORDS: *Ad hoc grid, Authorization, VOMS, attribute certificates*

INTRODUCTION

Grid computing uses Public Key Infrastructure (PKI) for building secure environment where digital certificates play significant role. In PKI, various kinds of certificates can be found: identity-based certificates which certify binding between public key and identity of its owner; authorization certificates which grant access permissions to an entity; and attribute certificates which bind a set of attributes to their holder.

Users in grid environments are usually organized in Virtual Organizations (VOs). A Virtual Organization is a collection of institutions and individuals that is defined according to a set of resource sharing rules. The VOs generally share resources and establish agreements with general facilities called Resource Owner offering resources (e.g. CPUs, network, storage) [1]. Certificates are utilized for identification, authentication as well as authorization processes in order to secure use the resources.

A proxy certificate used for a delegation process holds a special role in grids. In proxy delegation, [2] 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 proxy certificate contains a public and private key pair that is signed by the issuer certificate. The proxy certificate may also contain information about membership in particular VOs. The reason is a single sign-on: applications run by the user can authenticate themselves on behalf of the user using the proxy certificate, and thus there is no need for the user to provide a password every time the application is run.

In this article, a detailed explanation as well as mathematical description and sample certificates of our support authorization mechanism based on VOMS certificates in ad hoc grids is presented [3]. The mechanism can be used to build trust relationships during VO formation phase between grid entities even in cases when standard solutions have failed. The ad hoc grid environment, as described in detail in Section Ad hoc grid environment, 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. First we present a short overview of the ad hoc grid. Then the role of attribute certificates and VOMS service in grid security is described. Next section presents an implementation of the proposed mechanism into ad hoc grid environments as well as mathematical description of the mechanism. The paper is concluded with a short summary.

AD HOC GRID ENVIRONMENT

The definition of ad hoc grid can be found in different authors. Friese et al. in [5] 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 in [6] by Amin, Laszewski and Mikler as, "a distributed computing architecture offering structure, technology-, and control-independent grid solutions that support sporadic and ad hoc use modalities."

Some authors [7, 8] define an ad hoc grid environment as computing system with mobile devices. 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 three main characteristics of an ad hoc grid environment can be summed up as follows [4]:

- *Dynamics: The main characteristics of an ad hoc grid, belonging to the group of accessible grid, is its highly dynamic nature, which results from the frequently changing structure of underlying networks and VOs due to members switching on and off, member mobility, and so on [9].*
- *Resources: Ad hoc grids have more available resources (than for example MANETs), such as higher communication and computational capacity, more stable connections, etc. [10].*
- *Independence: As mentioned above, 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 users, i.e. that it is not possible to use the centralized administrative services as in traditional grids, each member 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 [11].*

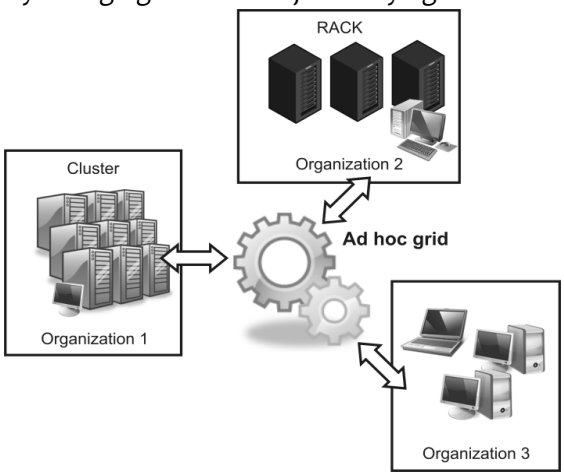

Figure 1. Ad hoc grid

AUTHORIZATION IN GRID AND VOMS SERVICE

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.

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 [6].

Various security mechanisms are practised in ad hoc grids, e.g.: every user has a set of trusted CAs; each policy fragment is systematically controlled and enforced by different users participating in the ad hoc grid; all members leave feedback ratings with the reputation server for the other members with whom they have completed transactions; techniques from MANETs and peer-to-peer networks are adopted to facilitate authentication for untrusted peers. We describe existing authorization mechanisms in traditional as well as ad hoc grid in detail for example in [3, 4].

In this Section we describe grid authorization mechanisms based on attribute certificates, because our mechanism benefits just from attribute certificates. Without loss of generality our mechanism will be demonstrated on VOMS attribute certificates.

One of the first authorization mechanisms of the Globus Toolkit [12] in VOs was a simple mechanism called "grid mapfile", where the resource owner makes decisions based on a list of all authorized grid users with their distinguished names (DN) mapped to local user accounts. This file can also serve as an access control list. The main disadvantage of the scheme is that authorization is boolean and there is no way to implement a fine grained authorization.

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 server is used to create and sign an attribute certificate enabling the user to gain access to grid resources and including the information about a user's VO [1, 13].

Every user in a VO is then characterized by a set of attributes included in attribute certificate by VOMS service, i.e. triple of the form (group, role, capability). The combined values of all of this triple form unique attributes, the so-called Fully Qualified Attribute Names (FQANs). A user may be a member of several groups, and he may hold a special role inside some of his groups. The VOMS user credentials provide additional role and capability data to application service providers which can then be used to make more fully-informed authorization decisions [14].

Note that attribute certificates are designed to provide information about attributes. Attributes are different data as e.g. subject's public key, but they are relevant to the subject. Attribute certificates bind attributes with the particular identity. Mostly there is a public key certificate attached to attribute certificate. Attribute certificates are signed by the attribute authority. Attribute certificates confirm that a user has the VO membership(s) and role(s) they are claiming to have.

Formally can be VOMS attribute certificate described as follow:

certatt = (cert(VO, ID(U), attr), sigAA(VO,ID(U),attr)) where cert is data part of certificate and VO is virtual organization, ID(U) is information about identity of certificate holder (i.e. FQAN) and attr are attributes bind with the holder; sigAA(VO, ID(U), attr) is digital signature issued by attribute authority (i.e. VOMS server).

VOMS CERTIFICATE-BASED AUTHORIZATION

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. Our mechanism allows other way based on VOMS certificates by which users can establish trust when previously used methods were not successful.

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 is similar to philosophy of decentralized trust model Web of Trust where PGP users build paths of trust among themselves in a distributed manner and the system allows users to specify how much trust to place in a signature by indicating how many independent signatures must be placed on a certificate for it to be considered valid [15].

Our 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 (pull model). 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.

The resource owner's list of trustworthy VOs can be selected from e.g. grid mapfile, if it is maintained by virtual organizations.

```
"/C=EU/O=/O=Organization A/CN=Alice" .voa
"/C=EU/O=Organization D/CN=David" .voa
"/C=EU/O=Organization B/CN=Bob" .vob
"/C=EU/O=Organization C/CN=Charlie" .voc
"/C=EU/O=Organization D/CN=Eva" .voc
```

Figure 2. Example of a grid mapfile used for a list of trusted VOs

Our authorization mechanism requires two main conditions:

(i) storing of VOMS attribute certificates on the side of each participant,

(ii) the trust is formed based on past authorized information included in VOMS attribute certificates, i.e. on previous VO membership of the users.

The first condition (i) requires the storing of VOMS attribute certificates from previous transactions. Since there is no central database of the certificates, each user builds its own storage of its VOMS attribute certificates as well as of all VOMS 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 VOMS certificates signed by particular VO. Building such storing space does not present a problem in a grid environment. For example, in the case described below, the size of a VOMS attribute certificate varies from 2386 to 2448 bytes, Figure 4. A similar philosophy of storage in grid environment can be found for example in the authorization system Akenti [16]. 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 included in VOMS attribute certificates and the trust decision of the resource owner is based on VOMS attribute certificates presented by a potential user.

The potential user should prove 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 VOMS attribute certificates.

The trust for an unknown potential user's VO is derived from the trust to trustworthy VOs. If the intersection of potential user's VO and resource owner's VOs is non-zero, the VOs from the intersection can be used to establish the trust. Number of certificates belonging to the VOs in intersection of the potential user's VO with the resource owner's VOs respectively must be greater or equal to the value k.

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 reflect the level of trust, the higher k allocates more rights, e.g. all the requested rights, the lower k allocates only particular rights.

Our mechanism does not assume any strictly pre-definite structure of trust, so such trust information is not in conflict with the independence of an ad hoc grid. 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 VOMS attribute certificates. If appropriate VOMS attribute certificates for confirmation of VO trustworthiness cannot be found on the potential user's side, the resource owner denies the access to the resource and other mechanisms of authorization and trust must be used.

For instance, in Figure 3, 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 listed as 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 unknown for the resource owner. The potential user for the VOx acceptance should send k co-member VOMS attribute certificates (k = 3) which belong to VOx as well as to the trustworthy resource owner's VOs, Figure 5. In our case, these are the VOMS attribute certificates of the members Alice, Bob and Charlie for their particular VOs and for VOx. 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 VOMS attribute certificates, one for VOb and one for VOc.

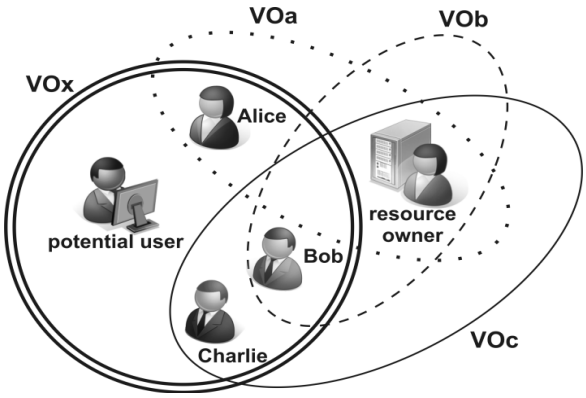

Figure 3. Intersection of VOs: VOa, VOb and VOc are trustworthy VOs for the resource owner. The trust for VOx is derived from them.

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.

-----BEGIN ATTRIBUTE CERTIFICATE-----

MIIGkDCCBXgCAQEwcKBuMGGkXzBdMQswCQYDVQQGEwJFVTEXMBUGA1UEChMOT3JnYW5pemFoaW9uIEExDjAMBgNVBAMTBUFsaWNlMSUwIwYJKoZIhvcNAQkBFhZhbGljZUBvcmdhbml6YXRpb25hLmV1AgkA8H7CsM8rdSegSzBJpEcwRTELMAkGA1UEBhMCRVUxDDAKBgNVBAoTA1ZPYTEMMAoGA1UEAxMDVk9hMRowGAYJKoZIhvcNAQkBFgt2b2FAdm9tcy5ldTANBgkqhkiG9w0BAQUFAAIBATAiGA8yMDExMDYyMTExMzc1NVoYDzIwMTEwNjIxMjMzNzU1WjBPMEoGCisGAQQBvkVkZAQxPzA9oBmGF1ZPYTovL3ZvYS52b21zLmV1OjE1MDExMCAEHi9WT2EvUm9sZT1OVUxML0NhcGFiaWxpdHk9TlVMTDCCBCswEgYKKwYBBAG+RWRkCwQEMAIwADAUBgNVHTcBAf8ECjAIMAYwBKACgAwCQYDVR04BAIFADAfBgNVHSMEGDAWgBQXHsbWBoG1CWvrXJ96n/wZ43egmDCCA9EGCisGAQQBvkVkZAoEggPBMIIDvTCCA7kwggO1MIICnaADAgECAgkAlW+FbpwEBpwwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCRVUxDDAKBgNVBAoTA1ZPYTEMMAoGA1UEAxMDVk9hMRowGAYJKoZIhvcNAQkBFgt2b2FAdm9tcy5ldTAeFwoxMTA2MjAyMDUwMzRaFwoyMTA2MTcyMDUwMzRaMEUxCzAJBgNVBAYTAkVVMQwwCgYDVQQKEwNWT2ExDDAKBgNVBAMTA1ZPYTEaMBgGCSqGSIb3DQEJARYLdm9hQHZvbXMuZXUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCw9ckAbch4JlJlCdXq6/EIs7VxTSwztfgixWstiOifZSFaUAMDjCzwUuYv7sAGMifw/SSiZVYW4x071zaZCPilrY+cPJg4oDQsGfJWAFftFQ79LUIwxQPy55uP9M65FKEWfyLaDYhHa6i8wjI1nrNUT/5ETBsCS98Om90Fgd6b1KWhopnZkzHP8LBmIBelDSBQ5zKAnjaG2y0IbvyEbwJa2KHPCtlZlrpCiKbxr+BhJX414AfjJavdrL7qyWftg2dWGF7lkT4BvqSxH7572DtpAgqlKfVX333KFtBpXG5vFTxZ/g7os0dSAb2AxGRm/7VRsC8mjMuxfdS7hmbedRrNAgMBAAGjgacwgaQwHQYDVR0OBBYEFBcextYGgbUJa+tcn3qf/Bnjd6CYMHUGA1UdIwRuMGyAFBcextYGgbUJa+tcn3qf/Bnjd6CYoUmkRzBFMQswCQYDVQQGEwJFVTEMMAoGA1UEChMDVk9hMQwwCgYDVQQDEwNWT2ExGjAYBgkqhkiG9w0BCQEWC3ZvYUB2b21zLmV1ggkAlW+FbpwEBpwwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAMWS9WhYvlw66BoU37FQej5XDIkkbbs6WtHITLcrIoRYxJpR7IJcdwRZfJInseZCg1JpixDkE25dzg3Xao07nktQSqLLs/k5X15hx5nXvKjAOk82PhtSTfkFlpUaOeoo1pnIsuWsgPTWvr/TQuBZ6ROzS214ANeerkQlGmHBD4X6ujOJ5lXR0ZzLPd5TzPHtk3riKAAO/baiONYlSPOGJ/7IDDOmu5/uHOliR+WevBZRSfG+gN1dq/PkRzQM99pnLFZNJuHPgEHmAb6aEUWtovWBWJvpfp2Ulpf6q8MZ5iEB41hvxeBkbOyS3nTd35YTBXakI3gu6ERoVcyCapuzVDTANBgkqhkiG9w0BAQUFAAOCAQEAbWucqklWsjIECNr3ALcoyA+RZ+pa9e+MF+f3hooslsrA+zJyByMeEUy8/a8R1rHcV7QZ4dwcp7s0MTTwGlsdng7Nk4t7tLIB9ENBVGnT9WOs+NVa/SCEfz5XkuSPUscU2WoiuYumqAUgakTqaAC3z8n7V2aW84lNBJI03mtyztikX3hVHdNI0UeoMWZJdHgxakxZooqowcB9OfLfAwEyfz+TQlfNs1y1bOYERKcv9qJGBz/XusdjaDzqgxguJwDg/5KbDoLo8QP/PiDqb6gS1+hugKSCroVIu50By8g/lY8aSCuQis76OYn6NQXh9ZohmJD6ApKazIlkFS132wHNDw==

-----END ATTRIBUTE CERTIFICATE-----

Figure 4. Sample of concrete VOMS attribute certificate encoded in a base64 format – Alice attribute certificate

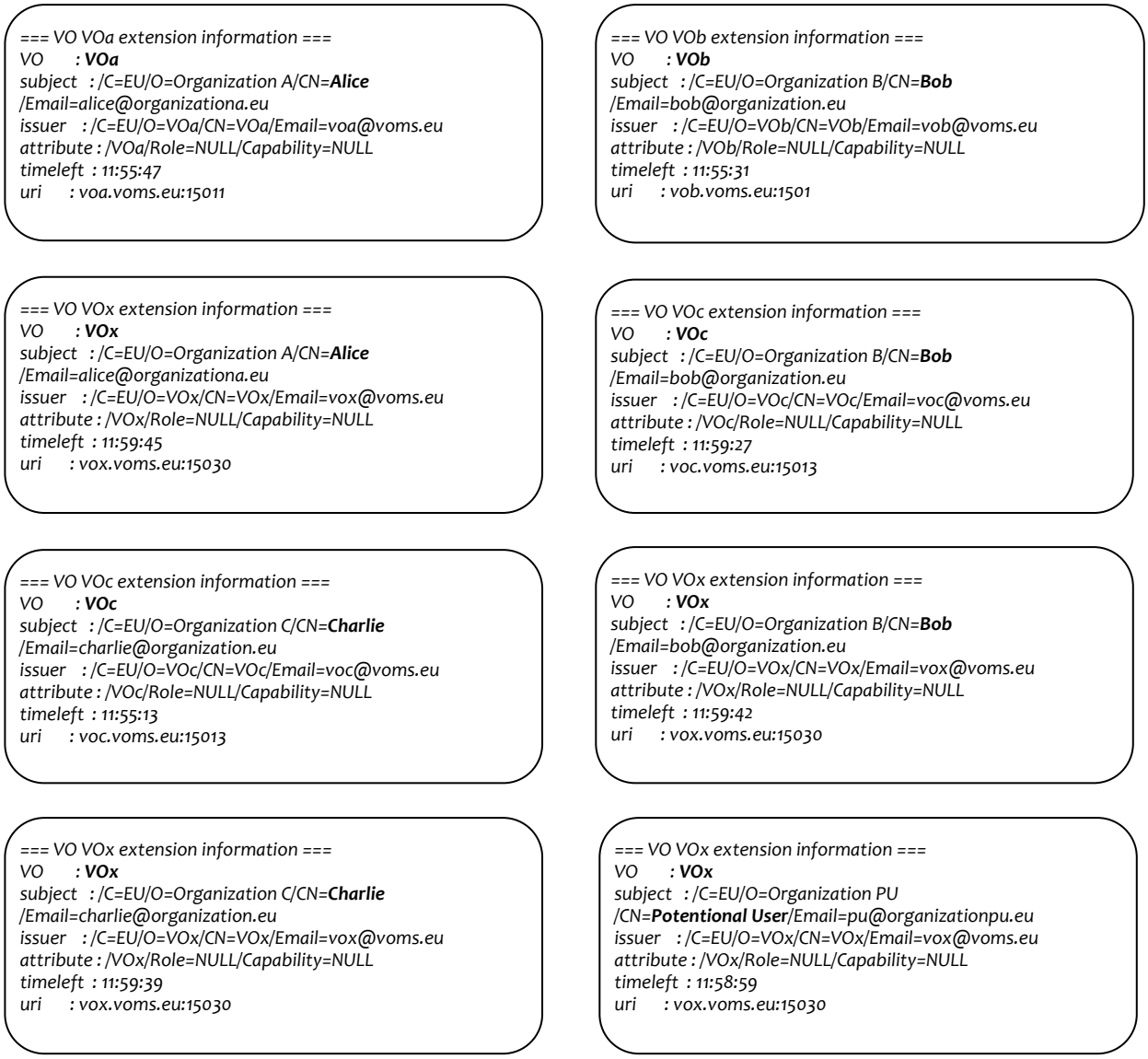

Figure 5. Example of VOMS attribute certificates in the mechanism

The authorization model can be mathematically described as follow:

Let M = {certatt1, certatt2,… certattm} be a set of attribute certificate possessed by potential user. Let VM = {VO1, VO2, … VOn} be a set of virtual organizations and let be a surjective function f: M → VM such that ∀VOj ∈VM ∃certatti ∈M, where virtual organization VOj is included in attribute certificate certatti. Let VR = {VO1, VO2, … VOr} be a set of trusted virtual organizations on the side of resource owner. Let k be required level of trust from the owner resources.

Let ∃virtual organization VOx such that VOx ∉VR ∧ VOx ∈ VM.

Than virtual organization VOx is trusted by intersection of virtual organizations with the level k for resource owner, if ∃ S, S ⊆M, where the cardinality of set S is |S| ≥ k and ∀certatti∈S there is a function {certatti} →{VOx} and furthermore, for ∀certatti∈S ∃certattj∈ M such that there is function {certattj} →VR and ID(U) of both certificates certatti and certattj is equal.

To prevent a compromising of a VOMS server database which could allow a malicious user to grant credentials with access rights for any service, a resource owner may require not only k different VOMS attribute certificates but also several less or equal k different VOs.

CONCLUSIONS

We have designed support VOMS certificate-based authorization mechanisms 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. Moreover, we have

mathematically described the authorization model with formalized VOMS attribute certificates as well as we have presented concrete samples of certificates in the scheme.

Further extension of the work involves mostly the revocation issue of the mechanism and detailed testing from different points of view [17,18] before being applied in practice.

REFERENCES

[1.] R. Alfieri et al., "From Gridmap File to VOMS: Managing Authorization in a Grid Environment," Future Generation Computer Systems, vol. 21, no. 4, 2005, pp. 549–558.

[2.] 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.

[3.] Huraj, L., Reiser, H.: "VO Intersection Trust in Ad hoc Grid Environments". In: Fifth International Conference on Networking and Services (ICNS 2009), Valencia, Spain, IEEE Computer Society, April 2009, pp. 456-461

[4.] Huraj L., Siládi, V.: "Authorization through Trust Chains in Ad hoc Grids", In: Proceedings of the 4th ACM EATIS annual international conference on Telematics and Informatics: New Opportunities to increase Digital Citizenship (EATIS '09), Prague, Czech Republic, June 2009, pp. 68-71, ISBN 978-1-60558-398-3.

[5.] 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.

[6.] 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.

[7.] 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.

[8.] 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.

[9.] H. Kurdi, M. Li, and H. Al-Raweshidy. A classifcation of emerging and traditional grid systems. IEEE Distributed Systems Online, 9(3), March 2008.

[10.] S. Zhao, A. Aggarwal, and R. D. Kent. Pki-based authentication mechanisms in grid systems. IEEE Int. Conference on Networking, Architecture, and Storage, pages 83-90, 2007.

[11.] K. Amin, G. von Laszewski, and A. R. Mikler. Hot service deployment in an ad hoc grid environment. Proc. of the IEEE 12th Int. Conference on Advanced Computing and Communications, 2004.

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

[13.] R. Alfieri et al. "VOMS: an Authorization System for Virtual Organizations" 1st European Across Grids Conference, Santiago de Compostela, Feb. 13-14, 2003.

[14.] V. Ciaschini, V. Venturi, A. Ceccanti. "The VOMS Attribute Certificate Format". OGF Draft, 11 Sep 2006

[15.] Khari, M., Shrivastava, G.: Public Key Infrastructure and Trust of Web Based Knowledge Discovery, In: International Journal of Computer Science and Security (IJCSS), Volume 5, Issue 3, 2011

[16.] 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.

[17.] Strémy, M., Eliáš, A.: Virtual laboratory communication. In: Annals of DAAAM and Proceedings of DAAAM Symposium. - ISSN 1726-9679. - Vol. 20, No. 1 Annals of DAAAM for 2009 & Proceedings of the 20th international DAAAM symposium "Intelligent manufacturing & automation: Focus on theory, practice and education" 25 - 28th November 2009, Vienna, Austria. - Vienna: DAAAM International Vienna, 2009. - ISBN 978-3-901509-70-4, pp. 0139-0140

[18.] Tanuska, P., Moravcik, O., Vazan, P.: The base testing activities proposal. In: Annals of DAAAM and Proceedings of DAAAM Symposium. ISSN 1726-9679, Vol. 20, No. 1, Annals of DAAAM for 2009 & Proceedings of the 20th international DAAAM symposium, November 2009, Vienna, Austria. DAAAM International Vienna, ISBN 978-3-901509-70-4, pp. 371-372.

ANNALS OF FACULTY ENGINEERING HUNEDOARA
– INTERNATIONAL JOURNAL OF ENGINEERING