VO-based Dynamic Security Associations in Collaborative Grid Environment

Yuri Demchenko[1], Leon Gommans[1], Cees de Laat[1], Martijn Steenbakkers[1]
Vincenzo Ciaschini[2], Valerio Venturi[2]

[1] *System and Network Engineering Group, University of Amsterdam*
Kruislaan 403, NL-1098 SJ Amsterdam, The Netherlands
{demch, lgommans, delaat, msteenba}@science.uva.nl
[2] *INFN CNAF, Viale Berti Pichat 6/2, 40121 Bologna, Italy*
{vincenzo.ciaschini, valerio.venturi}@cnaf.infn.it

Abstract

This paper discusses how the Virtual Organisation (VO) concept can be used for managing dynamic security associations in collaborative Grid applications and for complex resource provisioning. The paper contains both research part and discusses further development of the popular VO management software VO Membership Service (VOMS). The paper provides an overview of current practices in VO management in major Grid projects including operational procedures and supporting security middleware. The paper identifies open issues and basic requirements to the VO security functionality and services and suggests possible directions of further research and development. Proposed conceptual VO model and VO management framework provide a basis for consistent VO services definition and development to support different VO operational models. The paper intends to provide a framework for common understanding of the VO concept among Grid community and collaborative community and industry. The paper is based on experiences gained from the major Grid based and Grid oriented projects in collaborative applications and complex resource provisioning.

1 Introduction

Virtual Organisation (VO) and resource virtualisation are among the key concepts proposed in the Grid. According to the initial definition in one of the Grid foundational papers the "Anatomy of the Grid" [1], "Grid systems and applications aim to integrate, virtualise, and manage resources and services within distributed, heterogeneous, dynamic "virtual organizations".

The more detailed Grid definition includes such main components as distributed infrastructure, dynamics, virtualisation, and user-defined security – the components that provide a framework for coordinated collaborative resource sharing in dynamic, multi-institutional virtual organizations [1, 2].

Resources and services virtualisation together with provisioning are two major concepts in the Open Grid Services Architecture (OGSA) [3]. OGSA Security is built around VO concept and targeted for the security policies enforcement within a VO as an association of users and resources. VO provides a framework for inter-organisational and inter-domain trust managements. VO allows overcoming the problem of accessing by external users the enterprise internal network without affecting integrity of the enterprise security perimeter protected by the firewall. VO may run own security services, e.g. credential validation service, trust service, authorisation service, and attributes service but still many other services will remain in member domains and their authority needs to be translated into VO domain through established trust relations and shared semantics.

Although presenting a basic approach to understanding security services interaction in virtualised Grid environment, the VO definition in OGSA needs to be extended with more conceptual model and basic operational models required to support such typical use cases like project based collaboration, members' resource sharing or dynamic provisioning of complex multidomain distributed resources in general.

Current VO concept and existing practice lack a common theoretical foundation and as a result cause different understanding of the VO concept and functionality by different groups of potential adopters and users. In particular, the OGSA's vision of the VO and virtualisation is not provided with more detailed description of the VO functionality and operation required to support services and resources virtualisation and dynamic provisioning.

The goal of this work is to contribute to further development of the VO conceptual model and its application to typical collaborative applications and complex resource provisioning in open service oriented environment. One of intended paper goals is to provide a framework for common understanding the VO concept among Grid community and

collaborative community and industry.

The paper is organized as follows: Section 2 presents typical use cases of the collaborative applications and complex resource provisioning that require dynamic security associations and interdomain trust management and defines required basic VO functionality. Section 3 provides an overview and critical analysis of current VO usage practice in major Grid related projects. Section 4 provides analysis of how the VO concept can be used for managing dynamic security association from the conceptual point of view. It defines basic dynamic security associations of which the VO is currently used for the project oriented resource sharing and collaboration. Different VO operational models are suggested to reflect the specifics of typical use cases.

Section 5 attempts to formalise the conceptual VO model and define basic VO security services. Suggestions are given how the conceptual VO model maps to the related security services in current Grid middleware implementations. This section is actually based on the initial research about the VO functionality and identity management in [4] and intends to contribute to further VO concept development based on the OGSA VO definition [3].

Section 6 provides summary and suggests further development of the VOMS based VO management infrastructure to address basic requirements to VO functionality from major use cases analysed in section 2. One of goals is to make VOMS interoperable with existing identity and attribute management infrastructures and provide support for wide range of dynamic security associations. Suggestions are provided for the Optical Light Path Provisioning [5] and Open Collaborative Environment [6] and intended integration with the AAA Authorisation Framework [7, 8].

The proposed approach and solutions are being developed to respond to both common and specific requirements in the Collaboratory.nl (CNL)[1] and GigaPort Research on Network (GigaPort-RoN)[2] projects and are based on current experience in the EGEE[3] and LCG2[4] projects.

2 Collaboration and complex resource provisioning and required VO functionality

This section discusses basic VO security functionality required to support dynamic security services operation in two major use cases that benefit from using core Grid middleware services and infrastructure: to access complex experimental equipment in Open Collaborative Environment (OCE) and Optical Light Path Provisioning (OLPP) as an example of the general complex resource provisioning.

Effective use of advanced and unique experimental equipment for research and for production work requires complex infrastructure and collaboration of many specialists that may be distributed and span multiple organisations. Computer Grids and Web Services technologies provide a relevant platform for building a virtual collaborative environment.

Typical OCE use cases require that the collaborative environment:

- is dynamic since the environment can potentially change from one experiment to another,
- may span multiple trust domains,
- can handle different user identities and attributes/privileges that must comply with different policies (both experiment and task specific).

Security services are an important component of Grid based collaborative infrastructure to provide a reliable and secure operational environment that is capable of managing customers' and providers' resources. Collaborative applications require a sophisticated, multi-dimensional security infrastructure that manages secure operation of user applications between multiple administrative and trust domains associated with the particular experiment.

Proposed in [6] the Job-centric security model uses the Job description as a semantic document, created on the basis of a signed order (or business agreement). The document contains all the information required to run the analysis, including allocated resources, assigned users and roles, and a trust/security anchor(s) in the form of the resource and additionally the customer's digital signature. In general, such approach allows binding security services and policies to a particular job and/or resource and provides customer-controlled security environment with the job security context defined by a user/subject (i.e., their identity or secure credentials).

Job-centric security model is logically integrated with other stages and components of the collaborative (virtual) organisation managing the experiment stages. These stages include the initial stage of order creation and the main experimental stage that requires secure access to the instrument or resource.

OLPP is another important component of the distributed collaborative environment when dedicated high-speed communication channels are required for the experiment that may last from few hours to few months. OLPP provides an effective business model with current widely deployed optical network and dark optical cables. Further in the paper the OLPP use case will be also referred to as a complex resource provisioning as a more general definition.

OLPP and complex resource provisioning in general require creation of dynamic user-controlled resource allocation that may span multiple administrative and security domains. In comparison to the Job-centric security model where trust relations and consequently security associations are defined by an Agreement or Job shared by all coopering members, in OLPP user/customer may have agreement and consequently trust relations with only one, usually home, network provider. However, the provisional model must ensure that finally provisioned lightpath/resource is securely associated with the user credentials or user trust domain.

Typically provisioning process comprises of 4 steps:

[1] http://www.collaboratory.nl/
[2] http://ron.gigaport.nl/
[3] http://public.eu-egee.org/
[4] http://lcg.web.cern.ch/LCG/

resource lookup, complex resource composition (including options), reservation of individual resources and their association with the reservation ID/ticket, and finally provisioning or delivery. Reservation ID/ticket created at the reservation stage actually defines a security association between user/customer and service provider(s) that will exist for all period when the complex resource or service is used.

Currently the AAA Authorisation Framework and GAAA toolkit provide basic security services for the two discussed use cases. (It is suggested that) VO can be naturally/potentially integrated into distributed access control infrastructure and provide the following security functionality to support dynamic security association in collaborative applications and complex resource provisioning:

1) Dynamic trust management - VO as a security association created dynamically at the reservation/negotiation stage will provide a security context for other security operations such as Authentication (AuthN) and Authorisation (AuthZ) and also for general session management.

2) Attributes and metadata resolution and mapping - correct policy evaluation and combination in multidomain scenario requires either use of common attributes and metadata format and namespace or mapping between used formats and namespaces. Actual attribute and metadata mapping can be provided by trusted Identity Providers (IdP) and/or Attribute services belonging to the VO or VO trust domain.

3) Policy combination and aggregation – VO can provide a framework for the multiple policies combination that may be defined and managed by the VO common or federated policy. This may be especially important when individual policies may have potential conflicts at different levels and in different domains. In this case a VO creation procedure and policy should define how possible conflicts could be resolved.

4) VO itself must have flexible management infrastructure capable to operate in distributed multidomain and multi-organisational environment.

3 Virtual Organisations in Grid Applications

3.1 VO Management Practice in major Grid projects

In Grid applications and projects, VO is used as a framework for establishing project related resource sharing. The Grid Resource Centers (GRC) contribute some of their resources to the VO. Access to these shared distributed resources is provided based on the VO membership and other VO-related attributes like groups and roles.

Current VO management practice in LCG and EGEE projects provides a good example of the instant implementation of the VO concept. They have well-defined VO registration procedure, basic Security Policy, and simple Acceptable Use Policy. Major VO membership management tool is the VO Membership Service (VOMS) that provides VO-defined attributes for authorisation and also supports user registration procedure with the VOMS Admin server automated workflow.

The VO management framework in LCG/EGEE is defined by two main documents the Virtual Organisation Registration Procedure [9] and the LCG/EGEE Virtual Organisation Security Policy [10]. The first document lists the necessary steps and decisions a Virtual Organisation (VO) should take in order to get registered, configured and integrated in the LCG/EGEE infrastructure. This includes: naming the VO, VO integration into existing EGEE infrastructure from one of designated project bodies, setting-up a VO by selecting a site where to run the VO database (VODB) server and the Registration service/database (where the acceptance of the Grid Usage Rules by the user is registered); populating a VO, integrating VO into existing infrastructure, organizing support structure for the VO.

Another important document is the LCG/EGEE Virtual Organisation Security Policy that defines a set of responsibilities placed on the members of the VO and the VO as a whole through its managers. It aims to ensure that all Grid participants have sufficient information to properly fulfil their roles with respect to interactions with a VO, including VO Acceptable Use Policy - a statement which, by clearly describing the goals of the VO, defines the expected and acceptable usage of the Grid by the members of the VO, contact information for responsible people and URL of one or more VO Membership Servers.

Two large Grid infrastructure operated by Open Science Grid[5] (OSG) and TeraGrid[6] consortiums in US has interoperable VO management frameworks and operational procedures.

Current use of the VO is directly association with few major Grid projects and therefore VO is managed under the project administration. It is perceived that to become widely accepted, current VO implementation should be supported by more conceptual definition and be aligned with (yet to be developed) OGSA VO concept. First of all, it is related to the definition of the VO Agreement and VO Policy.

3.2 VO support in Grid middleware

Widely used in Grid applications the Virtual Organization Membership Service (VOMS) was been initially introduced in the framework of the EU project EDG, and currently it is being developed in the framework of the EGEE project [11, 12]. VOMS goal is to solve the problem of granting users authorization to access the resources at VO level, providing support for group membership, roles and capabilities.

In VOMS design, a VO is represented as a complex, hierarchical structure with groups and subgroups [11] what is required to clearly separate VO users according to their tasks and home institutions. A group is basically a set of users, which may also contain other groups. From the administrative point of view, management of each group can be independently delegated to different administrators. In general a user can be a member of any number of groups contained in

[5] http://www.opensciencegrid.org/
[6] http://www.teragrid.org/

the VO hierarchy.

Every user in a VO is characterized by the set of attributes defining their group membership, roles and capabilities in the scope of the VO that can be expressed in a form of 3-tuples (group, role, capability). The combination of all 3-tuple values forms a unique attribute, the so-called “Fully Qualified Attribute Name" (FQAN) [12], which is included as a text field into the VOMS Attribute Certificate, which is based on X.509 AC for Authorisation. However, its current use for Grid authorisation requires that the VOMS AC is included into the Proxy Certificate [13].

The VOMS system supports user requests for attributes with user server and client, and administrative tasks on VO management with administrative server and client [11]: VOMS infrastructure suggests that VO may have few VOMS servers with synchronised membership databases, but one VOMS server can serve multiple VO’s. Central membership database maintained by a VO must contain information/attributes for all registered VO members. Currently, only user attributes are stored in VOMS database. There is ongoing discussion about providing VO credentials to the resources as well.

Although current VO management and VOMS infrastructure are rather designed for long-term collaborative projects, VOMS posses all necessary functionality for creating ad-hoc dynamic VO associations. The issue remains how to consistently manage trust and authority in such a dynamic VO.

Current VOMS implementation can address a known privacy issue with user attributes stored in the VODB together with the user ID by registering user pseudonym or associating VO attributes with anonymous user and making further VOMS calls via local to user pseudonymous services or anonymiser. However, planned VOMS integration with the Shibboleth[7] infrastructure will benefit both solutions. More detailed information is provided in section 6.

Another VO management tool, the VOM Registration Service (VOMRS) has been developed and currently used by OSG Consortium [14]. VOMRS extends the VOMS system to include an easy-to-use interface for users to register with the system and request sign-in credentials associated with an authorized account in the application. VOMS's registration interface also asks the user to identify the institution to which they belong and the type of access they desire so that VOMS-based authorization data can be added. Requests are forwarded by email to an administrator, validated by an institutional representative, and the administrator uses administrative functions in the web portal to process requests. Users receive email notification when their accounts are ready for use.

When an account is created using VOMRS, the user data is stored in the VOMS database, which is used to automatically generate VOMS credentials for the user when they sign in. These credentials include authorization information in addition to the authentication information in the user's original credentials.

3.3 Privacy enhanced VO attributes management with GridShib profile

GridShib is an ongoing project that intends to integrate the Globus Alliance's Globus Toolkit[8] (GT) security infrastructure and widely used among universities and university federations the Shibboleth's Attribute Authority service (SAAS) to form a robust attribute infrastructure for campus environments to enable secure verification of user attributes for inter-institutional Grid users and also allow participants in multi-organizational collaborations to control the attribute information that they want to publish, share, and reveal to other parties through the user-controlled attribute release policy [15].

GridShib will enable Web Services access to Shibboleth services by using GT4 application integration tools. This will allow Shibboleth use for non-web-based applications. GridShib will support two basic attributes handling models in which attributes are requested by the resource (attribute pull) or obtained by the requestor prior to the request (attribute push) and bound to the real requestor identity. Two additional attribute handling models will allow attribute binding to the requestor’s pseudonymous identity or to an anonymous account. In both cases SAAS will provide a mechanism for the privacy enhancement in attribute handling.

4 VO and Dynamic Security Associations

This section attempts to review current VO concept and understand how the VO as an abstract concept and as a practical implementation can be used for federated and/or dynamic trust management. In other words, we will discuss relations between VO and dynamic security associations, i.e. which part of the VO organisation and operation is static (like Certification Authority (CA) and AttrAuth) and which can support dynamic associations (and dynamic trust management).

First of all we need to clarify one of widely used misunderstanding between VO as a virtual entity and dynamic processes and associations. To do it consistently we need to look at different types of security associations and their dynamics (or lifetime characteristics). In relation to this we can build the following list:

- **Session** – establishes security context in the form of session key that can be a security token or simple UID bound to secure credential or session ticket. Session may associate/federate users, resources and actions/processes.
- **Job/workflow** – this may be more long-lived association and include few sessions. Job or workflow is built around specific task that is defined either contract to perform some work or deliver product, or business process unit that also deliver some service and provides orchestration

[7] Shibboleth Project. - http://shibboleth.internet2.edu/

[8] Globus Toolkit. - http://www.globus.org/toolkit/

of many other processes. They may need to associated more distributed collection of users and resources for longer time required to deliver a final product or service. Job and workflow may contain decision points that switch alternative flows/processes. Security context may change during workflow execution or Job lifetime. Job description, as it is used in the Job-centric security model [6], may contain both user and resource lists and also provide trust anchor(s) (TA) and specify security policy. Job TA is derived from the requestor and the service trust relations established on the base of the contract to perform some job. Workflow TA can be implicitly derived from the parent process.

- **Project or mission oriented cooperation** – this type of association is established for long time cooperation (involving people and resources) to do some research, development or production but it still has some well-defined goals and area of activity and often criteria of mission fulfillment. This is actually the area of currently existing VO based associations.
- **Inter-organisational association or federation** – this type of association is built on long-term (often indefinite) cooperation agreements and may have a wide scope of cooperative areas. This is the area of inter-university associations which examples are InCommon[9] that uses Shibboleth as specially designed to support this kind of federations.

Comparing two last types of associations, we can suggest that for the VO type of federation the common membership service is typical and essential. However, its implementation can be either centralised like in VOMS or distributed like it is intended in the GridShib profile.

Proposed above classification allows to assume that all identified types of associations will have its place and use in the future responding to different goals and tasks. Another suggestion that can be made from the above discussion in the context of user controlled service provisioning (UCSP) is that Job-centric/VO-based associations may scale to each other and consequently use each other's technical infrastructure and tools by adopting the dynamics to their specific tasks.

Now we will try to identify possible VO operational models depending on more detailed analysis of the major service provisioning use cases that require dynamic security associations management

When considering the use of VO for trust and attributes management, we should refer to the conclusion made in the VO overview section (section 3) that current VO creation practice is rather complicated and formal procedure. VO creation is normally initiated by one of organisational or business/project entity and has a specific goal and mission. VO can be created for the project based collaboration, members' resource sharing or dynamic provisioning of complex multidomain distributed resources in general. VO concept can be also used for general purpose user associations.

[9] http://www.incommonfederation.org/

VO attribute or membership service is used for trusted attributes brokering between (member) organisations when requesting resources or services from the VO members or their associates. However, VO operation will differ depending on what are the VO associated members and how the VO membership service is used in VO related activities or services.

In this context three basic and one additional VO operational models can be defined:

- **User-centric VO (VO-U)** that manages user federation and provides VO related attribute assertions based on user identity/credentials.
- **Resource/Provider centric VO (VO-R)** that supports provider federation and allows SSO/access control decision sharing between resource providers.
- **Agent centric VO (VO-A)** that provides a context for inter-domain agents operation, which process a request on behalf of the user and provide required trust context to interaction with the resource or service.
- **Project centric VO (VO-G)** that combines User centric and Provider centric features what actually corresponds to current VO use in Grid projects.

Although in different applications and use cases VO operations will differ in sense of providing primary association of users, resource providers or services providers the VO management infrastructure will need to have almost the same set of services. The above classification should help to understand how major security services will operate in each of the different types of VO.

User-centric VO-U manages user federation and provides attribute assertions on user (client) request. For this purpose, VO-U maintains Attribute Authority Service (AAS) that receives requests from user clients and provides VO member attribute certificates or other type of attribute assertion. VOMS/AA can also validate user credentials on request from services. However, this is the user who presents attribute credentials to the service in order to obtain access control permission. VO Attribute service is the central service for this type of VO. This can be considered as current operational model for the VOMS in Grid application. GridShib profile will allow decentralisation of attributes management and also user controlled attribute release.

Resource/Provider centric VO-R supports provider federation and allows Single-Sign-On (SSO) and access control decision sharing between VO members, i.e. resource providers. It is logically that all services in the VO-R association can accept the VO AuthZ service decision once issued for the user on their request. If the user wants to access multiple services in the VO-R s/he can use obtained access granting ticket as a SSO credential, however services may need to validate presented credentials/ticket with the VO AuthZ and AuthZ services.

Agent centric VO-A provides a context for inter-domain agent operation. In this VO model the agent acts as a representative and a broker of the trust and other services for the specific domain. Agents are considered more independent in the VO-A than users or providers in other models VO-U

and VO-R. Agents may have central attribute or certificate service but in more specific for the VO-A model case they will maintain mutual trust relations (which initial establishment for the time being is out of scope for this study).

Project centric VO-G (as originated from Grid projects) can be introduced to reflect typical use case when a VO is established to support user cooperation in the framework of the long-running project and to overcome existing/legacy organisational boundaries. VO-G associates both users and resources and actually combines two identified earlier models VO-U and VO-R. It maintains central VO membership/attribute service and may run also VO-wide security services such as AuthN/IdP/SSO and AuthZ.

There may not be clear difference in real life VO implementations to which operational model they adhere but proposed abstraction will help to more flexibly design supporting middleware security services. For example, it can be suggested that current VOMS based VO in Grid will evolve from currently used VO-U model to more appropriate VO-G model.

The major motivation behind defining basic VO operation models is to define possible profiles for the VO security services as well as suggested gateway services to interact with other infrastructural components.

Benefit of using VO based trust and attribute management/brokering is that VO can be created and used as a dynamic association for wide range of duration given the VO as a concept that can potentially combine virtualisation and dynamic.

5 VO management Framework

5.1 Basic functionality and available technologies

Virtual Organisation is defined in OGSA as a key concept for operation and managing Grid services [3, 4]. VO supplies a context to associate users, resources, policies and agreements when making and processing requests for services related to a particular VO.

VO management service should provide the following functionality: a) registration and association of users and groups with the VO; b) management of user roles; c) association of services with the VO; d) associating agreements and policies with the VO and its component services. They should support the VO operation during the whole VO lifecycle including creation, operation and termination stages. Depending on implementation the VO management service can be centralized or distributed relying on related services in member organisations.

Implementing and using VO concept requires a mechanism to reference the VO context and associate it with the user request. VO membership service (VOMS*) contains authoritative information about the entities and services associated with the VO, or VO's associated with the particular entity or user. Prior to VO creation there must be a formal agreement established between the VO members. In this way VO follows the same procedure as real organisation and in case of business oriented VO this stage may require relevant legal basis for establishing and operating such a VO. WS-Agreement [16], WS-Trust [17], WS-Policy [18], and WS-Federation [19] can provide the initial technological platform for dynamic VO creation.

In order to securely process requests that traverse between members of a VO, it is necessary for the member organisations to have established trust relations. These trust relations may be direct or mutual, or established via intermediaries like VO Trust Management Service.

In wider VO and Grid infrastructure there may be a need to establish a VO Registry service that will provide a VO reference/ID registration and resolution and can also keep VOMS public credentials. Current LCG/EGEE VO naming and registration procedure [9] actually allows using DNSSEC [20] for populating VO together with its public key that can be used for initial trusted introduction of the VO and secure session request by the requestor.

5.2 VO Security Services and Operation

VO can be established according to a well-defined procedure and based on common agreement between member organisations to commit their resources to the VO and to adhere to common policy that may be simple enough but not to contradict to the local security policies at member institutions. And opposite, if some specific enforcement is required by a specific VO, it should be also supported by local policies. Otherwise VO should provide direct individual membership for users which home organisation (HO) credentials can not be used or not trusted.

VO establishes own virtual administrative and security domains that may be completely separate or simply bridge VO members' security domains. This is required to enable secure service invocations across VO security domain but also requires coordination with the security policies in member organisations.

The following security services and related functionalities are required for the VO:

1) Identity Management Service, normally provided by the Identity Provider (IdP) and may also include Identity Federation service that provides federated identity assertions for users or resources, including Pseudonymous services as a particular case.

2) Attribute Authority Service (AAS, e.g. VOMS) that issues attributes bound to user or resource identity that primary can be used for authorization decision when accessing VO resources or services.

3) Authorization service to enforce access control to the resource or service based on entity's attributes/roles and authorisation policies.

4) Policy Authority to provide VO-wide policies related to authorisation, trust management, identity federation, mapping of identities, attributes and policies

5) Trust management service that may include CA and associate PKI management services, and Security Token

Services as defined by WS-Trust. VO Agreement provides initial base for building trust relation inside VO.

VO can also have other services, which are important for it's functioning such as logging, accounting, auditing/non-repudiation, etc. Physically, all VO services may be provided by member organisations on behalf of the VO and be distributed. In case of distributed VO membership or Attribute service, mapping between user/requestor local identities and attributes can be provided either by IdP or AAS.

VO is normally created for a specific task, which however may be long lived. A VO lifecycle includes stages of creation, operation and termination. It is perceived that an initial VO is created by human individuals or organisations (in fact, real or virtual, depending on agreement and policy) on the base of an agreement between all member organisations and set of policies that VO must adhere.

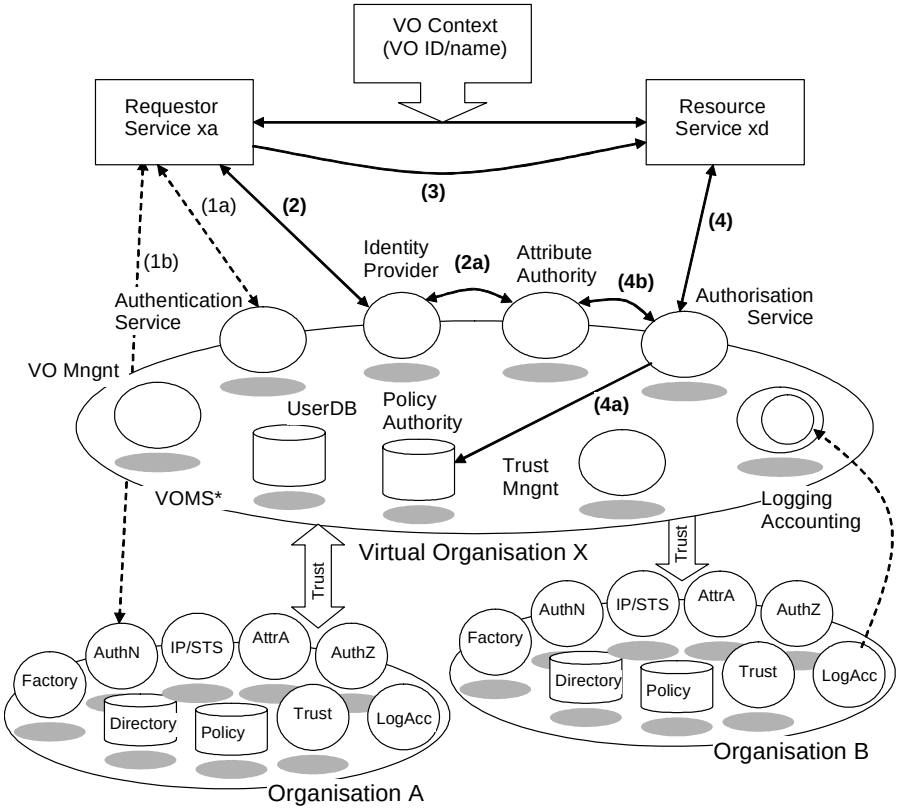

Fig. 1. Interaction of the VO security services when processing a request inside VO.

Figure 1 illustrates relationship between Virtual Organisation X and two member organisations A and B, which can be either real or virtual. VO X has been created to perform some task or provide some service(s) for designated group of users that constitute VO user community. VO established its own administrative and trust domain. Some of the users of organisations A and B may become the members of the virtual organisation; some of the services provided by member organisations may become VO services. Based on their VO identity or attributes, the VO users and services can interact in the trusted manner using VO security services.

The picture shows basic services representing VO security infrastructure that provides reliable, secure and accountable VO operation, and illustrates in details how the request from the service xa (that actually represents service Aa from the member organisation A) to the service xd (representing service Bb from the member organisation B) is handled using VO context. To become an active entity in the VO, a service or user must authenticate themselves to the VO AuthN Service (step 1a) or present AuthN assertion from the requestor home organisation A (step 1b). Then, the requestor service requests a security token from the Identity service (step 2), this step may also include obtaining specific attributes for the service xd from the Attribute Authority (step 2a). Now the security token together with the obtained attributes may be presented to the target service xd (step 3). It's suggested that the resource will trust security credentials issued by the VO's Identity service and presented in the request, otherwise it may request their confirmation by the issuer. Before granting or denying access, the resource may request VO Authorisation service to evaluate user request and presented credentials against access control policy that may be obtained from the Policy Authority (steps 4, 4a, 4b).

6 Conclusion and Summary

VOMS already has a wide user community and a proven implementation among Grid projects and related scientific community. However, VOMS has a wider potential and it can provide the functionalities for managing dynamic security association and related security services in dynamic resource provisioning and open collaborative environment that are already required in the industry and in wider university/academic communities. In fact, VOMS designers have already the intention to support these use cases, and the requirements coming from this paper will be included in the development process.

Another intended goal of the paper is to suggest interoperation and integration framework for VOMS and AAA Authorisation Framework that is currently being developed to provide access control service for the Open Collaborative Environment and Optical Light Path Provisioning described in section 2 as basic use cases.

The results presented in this paper are the part of the ongoing research and development of the generic AAA Authorisation framework in application to user controlled resource provisioning and collaborative resource sharing conducted by the System and Network Engineering Group in the framework of different EU and nationally funded projects including EGEE, NextGRID, Collaboratory.nl, and GigaPort Research on Network. All of these projects are dealing with the development, deployment or use of the Grid technologies and middleware infrastructure platform providing a scope of different use cases for both the Grid and the AAA.

It is important to mention that VOMS development in INFN is allied and coordinated with other projects and tools for authorisation and policy management such as G-PBox [21] and recommended in GGF Authorisation Attributes profile [22].

The paper provides an overview of current practice with the VO management at the organisational level and its support at the Grid security middleware level. It identifies the open issues and basic requirements to the VO security functionality and services and discusses possible areas of research and development, in particular, related to the VO management concept, dynamic interdomain trust management for user-controlled applications, multi-domain policy decision and user attributes management.

Based on suggested VO definition as a framework for managing dynamic security associations of users and resources in service oriented environment, the paper identifies a few basic VO operations models depending on what the VO primary goal to associate users, resources, or agents as active business intermediaries.

Proposed conceptual VO model addresses VO management issues and VO security services operation and can be used as a conceptual basis for developing VO management tools to support required creation, management and termination of dynamic security associations.

The authors believe that the proposed approach and ideas will provide a good basis for further wider discussion how the VO concept can be developed to provide a more flexible framework for identity and attributes management in dynamic task oriented virtual associations. There is also an intention to contribute this work to the Global Grid Forum (GGF)[10] standardisation process as a practical input from such application areas as complex resource provisioning and collaborative resource sharing.

7 References

[1] Foster, I., Kesselman, C. and Tuecke, S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International Journal of Supercomputer Applications, 15 (3). 200-222. 2001.

[2] Foster, I., Kesselman, C., Nick, J. and Tuecke, S. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. Globus Project, 2002. www.globus.org/research/papers/ogsa.pdf.

[3] The Open Grid Services Architecture, Version 1.0 – 29 January 2005. - - http://www.gridforum.org/documents/GFD.30.pdf

[4] Demchenko Yu. Virtual Organisations in Computer Grids and Identity Management. – Elsevier Information Security Technical Report - Volume 9, Issue 1, January-March 2004, Pages 59-76.

[5] B.Oudenaarde, et al. “Grid Network Services: Lessons and proposed solutions from Super Computing 2004 demonstration”, GGF Draft. - https://forge.gridforum.org/projects/ghpn-rg/document/Grid_Network_Services_in_the_SC04_Demonstrator/en/1

[6] Job-centric Security model for Open Collaborative Environment, by Yuri Demchenko, Leon Gommans, Cees de Laat, Bas Oudenaarde, Andrew Tokmakoff, Martin Snijders. - Proceedings 2005 International Simposium on Collaborative Technologies and Systems (CTS2005). - May 15-19, 2005, Saint Louis, USA. - IEEE Computer Society, ISBN: 0-7695-2387-0. - Pp. 69-77.

[7] RFC 2903, Experimental, "Generic AAA Architecture",. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence, August 2000 - ftp://ftp.isi.edu/in-notes/rfc2903.txt

[8] RFC 2904, Informational, "AAA Authorization Framework" J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence, August 2000 - ftp://ftp.isi.edu/in-notes/rfc2904.txt

[9] Virtual Organisation Registration Procedure. By Maria Dimou, Ian Neilson. - https://edms.cern.ch/document/503245/

[10] http://www.gridforum.org/

[10] LCG/EGEE Virtual Organisation Security Policy. Version 1.1, by Ian Neilson - https://edms.cern.ch/document/573348/
[11] Virtual Organization Membership Service (VOMS) project homepage - http://infnforge.cnaf.infn.it/voms/
[12] VOMS Attribute Certificate for Authorisation. - http://infnforge.cnaf.infn.it/voms/AC-RFC.pdf
[13] RFC 3820, Standard Track, "Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile" S. Tuecke, V. Welch, D. Engert, L. Pearlman, M. Thompson, June 2004 - ftp://ftp.isi.edu/in-notes/rfc3820.txt
[14] VOMRS - Virtual Organization Management Registration Service - http://www-unix.grids-center.org/r6/ecosystem/security/vomrs.php
[15] GridShib - A Policy Controlled Attribute Framework - http://grid.ncsa.uiuc.edu/GridShib/
[16] Andrieux, A. et al, "Web Services Agreement Specification (WS-Agreement)," August 2004, available from https://forge.gridforum.org/projects/graap-wg/document/WS-AgreementSpecification/
[17] Web Services Trust Language (WS-Trust) - ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf
[18] Web Services Policy Framework (WS-Policy). Version 1.1. - http://msdn.microsoft.com/ws/2002/12/Policy/
[19] Web Services Federation Language (WS-Federation) Version 1.0 - July 8 2003 – http://msdn.microsoft.com/ws/2003/07/ws-federation/
[20] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, "Resource Records for the DNS Security Extensions", RFC4034. - http://www.rfc-archive.org/getrfc.php?rfc=4034
[21] V.Ciaschini, A.Ferraro, A.Ghiselli, G.Rubini, R.Zappi, "G-PBox: A Policy framewrok for Grid Environments", Chep 2004
[22] M. Thompson, V. Welch, M. Lorch, R. Lepro, D. Chadwidk, V. Ciaschini, "Attributes used in OGSI Authorisation", GFD-E.057, Global Grid Forum.