Policy Based Access Control in Dynamic Grid-based Collaborative Environment

Yuri Demchenko
University of Amsterdam
demch@science.uva.nl
Leon Gommans
University of Amsterdam
lgommans@science.uva.nl
Cees de Laat
University of Amsterdam
delaat@science.uva.nl

Andrew Tokmakoff
Telematica Instituut
Andrew.Tokmakoff@telin.nl
Rene van Buuren
Telematica Instituut
Rene.vanBuuren@telin.nl

ABSTRACT

This paper describes the development and design of a flexible, customer driven, security infrastructure for Grid-based Collaborative Environments. The paper proposes further development of the access control model built around the service or resource provisioning agreement (e.g., experiment or project) that is used as a basis for an instant access control policy definition and virtual association of users and resources. Workflow management technology is considered as a solution for dynamic security context management during the whole experiment lifetime. The paper analyses required functionality and suggests extensions to the generic AAA Authorisation framework to support complex collaboration scenarios in the dynamic virtualised environment. The paper provides implementation details of using XACML for fine grained access control policy definition for complex resources and team-based roles management, and SAML for secure credentials exchange. In addition, the paper discusses how the Virtual Organisations (VO) concept can be used for experiment-based dynamic security associations management. Proposed technical solutions are intended to be compatible and interoperable with current implementation of the Grid security middleware in Globus Toolkits and gLite. The paper is based on experiences gained from the major Grid based and Grid oriented projects in collaborative applications and complex resource provisioning.

KEYWORDS: Grid-based Collaborative Environment, Policy based access control, workflow, RBAC, SAML, XACML

1. INTRODUCTION

Effective use of complex experimental and research equipment involves many specialists for both supporting its normal operation and processing experiment results and requires corresponding infrastructure that is created for the purpose of running experiment and may span multiple organisations. Emerging Computer Grid and Web Services [1, 2] technologies provide a good basis for building such a Grid-based Collaborative Environment (GCE) that allows dynamic association of resources and users into virtual organisations or laboratories. Such a virtualisation of resources and users can be created dynamically based on experiment or business agreement and terminated after the experiment is finished.

For the recent period, the Grid middleware has experienced active developed in the framework of large international projects such as EGEE[1], OSG[2] and Globus Alliance[3] and reached production level of maturity, but it still remains more focused on computational resources and tasks management. Grid middleware provides common communication/messaging infrastructure for all resources and services exposed as Grid or Web services and allows uniform security services application at the service container or messaging level. This significantly simplifies development of GCE applications and allows developers to focus on application specific tasks such as providing advanced business process management and complex application specific services delivery.

In GCE, security services and infrastructure play important role in providing reliable and secure resources/instruments access and services delivery. This

[1] http://public.eu-egee.org/
[2] http://www.opensciencegrid.org
[3] http://www.globus.org/

paper describes the experience of developing a flexible, customer driven, security infrastructure for dynamic GCE. It proposes further development of the Job-centric security model built around the service or resource provisioning agreement (e.g., experiment or project) proposed in [3] and being developed in the framework of the Collaboratory.nl[4] project (CNL). Although proposed solution can provide a general, experiment-defined security context for all security services operation, there is no possibility to change this context during the experiment lifetime.

The paper looks into further improvement and automation of management of all experiment components and supporting services during the whole experiment lifetime with the workflow management technologies, in particular, for dynamic security context management and as a basis for an instant access control policy definition.

The paper is organized as follows. Section 2 provides short information about recent developments in the CNL project, discusses experiences with the implementation of the Job-centric security model, and provides motivation for further its extension to using workflow management technology. Section 3 explains how authorisation service operates in the Grid/Web Services based collaborative environment. Section 4 describes how two complementary standards XACML and SAML can be used to provide interoperable fine-grained policy based access control. Suggestions are given for using special XACML profiles for complex resources control and for team-based access rights delegation.

Section 5 provides suggestions how the Virtual Organisation (VO) concept can be used for creating dynamic security associations of users and resources based on the collaboration or experiment agreement. This should allow establishing inter-organisational trust relations and providing VO members access to internal resources without changing organisational security policy.

The proposed approach and solutions are being developed to respond to both common and specific requirements in the Collaboratory.nl and are based on current experience in the EGEE project. The proposed approach and solutions can also be used for other use cases that require distributed dynamically invoked and managed access control infrastructure using Grid and Web Services middleware.

[4] http://www.collaboratory.nl/

2. USING WORKFLOW CONTROL FOR EXPERIMENT RELATED SECURITY CONTEXT MANAGEMENT

The presented work continues with further development of the Job-centric customer driven security model for Open Collaborative Environment proposed in [3, 4]. The paper [3] provided introduction into proposed Job-centric security model and discussed such important issues as performance optimisation issues, trust management in a distributed access control infrastructure, multiple policy evaluation and multiple authorisation decision combination.

Proposed solutions have been developed in the framework of the industry funded Collaboratory.nl project which after successful Demonstrator phase entered into the prototype design stage. The CNL demonstrator was built using Globus Toolkits platform (version 3.2) that provided access to analytical instruments as Grid services. CHEF (recently merged into Sakai[5] project) was used as a collaborative portal and Kizna SyncShare[6] server for real-time collaborative jobs/tasks management.

Continuing with the general design approach of using Grid and Web Services platform the project is in the process of re-engineering some components to ensure current compatibility with and gradual migration to the Grid architecture and middleware. This is, first of all, to be achieved by using standard interfaces, protocols, messages and data formats.

Typical GCE use cases requires that the collaborative environment:

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

Currently these problems are addressed in a manual way by manually configuring and managing user accounts and instruments what is resulted in a slow adaptation of the working space, high administrative overhead and complex management.

Collaborative applications require a sophisticated, multi-dimensional security infrastructure that manages secure operation of user applications between multiple

[5] http://www.sakaiproject.org/
[6] http://www.kizna.com/products_sync.html

administrative and trust domains associated with the particular experiment.

Current job definition in the CNL Job-centric security model provides a user access context during the experiment/job execution what works well for simple experiments. For complex experiments there is a need to execute and/or manage a complex workflow that may also change the scope or context for some security services (including access control policies) at different experiment stages. This means that workflow management framework and tools for experiment-centric, customer-driven GCE should allow also management of the security context and callouts to security services.

Recently, technologies and tools for managing scientific workflow and business processes are attracting great interest among e-Science community and in the business world. The paper [5] provides comprehensive overview and analysis of available Scientific Workflow Management Systems (SWMS) and their use for experiments automation. Most of SWMS have been developed and used in the framework of different e-Science research projects and are often oriented on some specific scientific research areas.

With the Web Services development, industry has been focused on developing the business process management and execution framework for Web Services. Workflow description standardisation is currently ongoing in the framework of the OASIS Web Services Business Process Execution Language (WSBPEL) TC based on early proposed BPEL4WS standard by leading industry players such as IBM, Microsoft, Oracle, and others [6, 7]. Currently available BPEL design and execution tools can simplify major part of the experiment automation.

Figure 1 shows the content of the Experiment description created by the experiment owner Principal Investigator (PI) as a semantic object on the base of signed agreement. It contains all the information required to run the analysis, including the Experiment ID, assigned users and roles, and a trust/security anchor(s) in the form of the resource and additionally the customer's digital signature. The experiment description is used to provide experiment dependent configuration data for other services to run experiment and manage dynamic security context, in particular, VO membership service to manage users and their roles, policy (or set of policies), and workflow that will drive the experiment execution and orchestrate all involved services.

It is investigated that the Order document could be described using WS-Agreement (WSA) format [8] to have potential compatibility with the Grid Distributed Resource Management Application framework (DRMAA) [9]. Experiment description exists in a form of XML document and can be used as a scope for developing workflow with the standard workflow design tools.

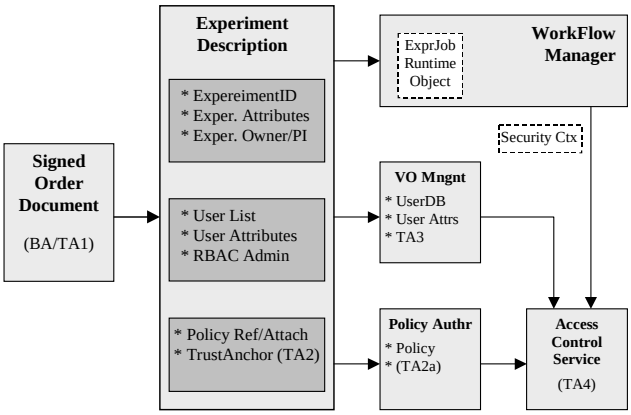

Figure 1. Workflow and security context in GCE

In general, such approach allows binding security services and policies to a particular experiment and/or resource and provides customer-controlled security environment with the root of trust defined by a customer (i.e., their identity or private key, based on Trust Anchor TA1). All other security services and related documents may have additional explicit trust anchor, such as TA2 for PI controlled Experiment description and TA3 and TA4 for security services.

Experiment-centric and workflow driven security model is logically integrated with other stages and components of the collaborative (virtual) organisation managing the experiment stages. VO can provide a good platform/solution for managing dynamically established trust relation between member organisations in the process of performing a specific experiment, using the fact that VO is created on the basis of cooperative agreement between participating organisations.

3. AUTHORISATION SERVICE OPERATION IN THE GRID-BASED COLLABORATIVE ENVIRONMENT

Fine-grained access control in typically interactive services in GCE can be achieved with the Role Based Access Control (RBAC) authorisation model which generally consists of such major functional components as Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Authority (PAP) [10]. In RBAC, user/requestor access rights are defined by roles in a form

of user attributes, separately managed access control policy contains rules that define what roles are allowed to do what actions on the resource.

Figure 2 below shows main interacting components and services participating in the service request evaluation in a typical Grid or Web Services based collaborative environment. Resource or Service is protected by site access control system that must rely on both Authentication (AuthN) of the user and/or request message and Authorisation (AuthZ) that applies access control policies against the service request. It is essential in such a service-oriented model that AuthN credentials are presented as a security context in the AuthZ request and can evaluated by calling back to AuthN service and/or Attribute Authority (AttrAuth).

The Requestor requests a service by sending a service request ServReq to the Resource's PEP providing as much or as little information about the Subject/Requestor, Resource, Action as it decides necessary according to the implemented authorisation model and (should be known) service access control policies.

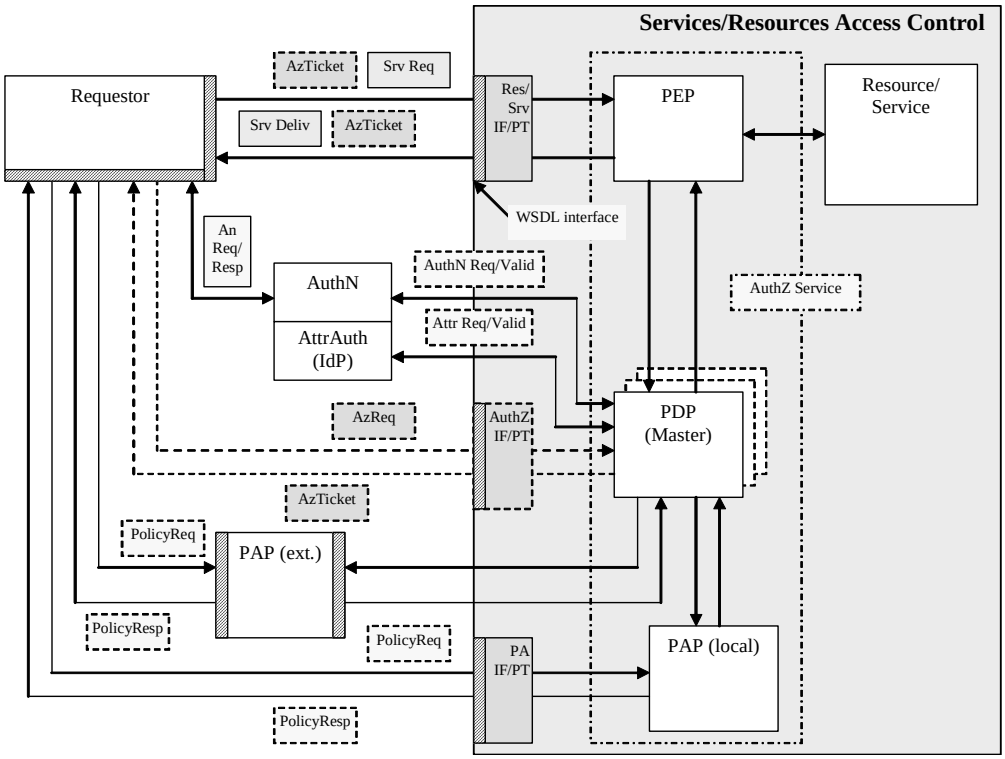

Figure 2. Main interacting components involved into access control in the typical Grid-based collaborative application

In a simple scenario, the PEP sends the decision request to the (designated) PDP and after receiving a positive PDP decision, relays a service request to the Resource. The PDP identifies the applicable policy instance and retrieves it from the Policy Authority (local or external), collects the required context information and evaluates the request against the policy. During this process, it may need to validate the presented credentials locally, based upon pre-established/shared trust relations, or call external Authentication and Attribute Authorities that can be also a function of the Identity Provider (IdP).

In the distributed access control infrastructure in order to optimise performance the Authorisation service may also issue authorisation tickets (AuthzTicket) that confirm access rights, are based on positive decision of the Authorisation system and can be used for granting access to the following similar requests that match an AuthzTicket. To be consistent, AuthzTicket must preserve full context of the authorisation decision including AuthN context/assertion and policy reference.

A typical access control use-case may require combination of multiple policies and multi-level access control enforcement which may take place when

combining newly-developed and legacy access control systems into one integrated access control solution. The GCE experiments may apply different policies and require different user credentials depending on the experiment stage.

The paper [3] provides an analysis and suggestions how instant service request evaluation can be done against multiple policies by combining policies or combining PDP/PEP, however this approach requires additional processing in case of complex resource provisioning and stateful requests processing. Additional integration of the access control system with the experiment flow management discussed in this paper will allow dynamic security context management and may simplify multiple policies management..

4. EXTENDING GAAA AUTHORISATION FRAMEWORK FOR DYNAMIC COLLABORATIVE APPLICATIONS

Described above functionality can be provided by the GAAA Toolkit (GAAA_tk) being developed by the System and Network Engineering (SNE) Group at the University of Amsterdam [11]. GAAA_tk provides basic functionality for the Generic Authentication, Authorisation, Accounting (GAAA) Authorisation framework described in [12, 13]. It features two basic profiles: an RBAC profile for collaborative applications specifically targeted for fine-grained team-oriented access control to shared resources, and a GAAA-P profile for complex resources/services provisioning in multidomain distributed service-oriented environment.

To support dynamic security context change, the GAAA_tk should provide advanced configuration management capability based on the generic AuthZ service operational model. Adding workflow processing functionality in GAAA-P profile in combination with rich policy evaluation capability in GAAA-RBAC profile will allow for complex multi-domains policies evaluation and complex provisioning algorithms execution.

4.1. GAAA-RBAC Implementation with the GAAA Toolkit

Figure 3 shows the GAAA_tk structure that contains the following functional components related to two basic profiles GAAA-RBAC and GAAA-P:

- GAAAPI that provides all necessary functionality for communication between PEP and PDP and providing security context for service request evaluation against service (access) policy and includes
  - Namespace resolver to define/resolve what policy and what attributes should be used for the request evaluation;
  - Triage and Cache that provide initial evaluation of the request including validity of provided credentials; this functionality is used for AuthZ tickets/tokens handling and AuthZ session management by evaluating a service request against provided AuthZ ticket/token claims;
  - Attribute resolver and Policy Information Point (PIP) provide resolution and call-outs to related authoritative Policy Authority Points (PAP) and Attribute Authority Service (AAS) which can be a part of general Identity Provider service (IdP);
- GAAA-RBAC subsystem provides GAAA-RBAC profile functionality and basically includes PEP, PDP and GAAAPI with related Application Specific Modules (ASM);
- GAAA-P subsystem includes GAAA-RBAC subsystem used for general policy evaluation and adds flow control with the Flow Control Engine (FCE) and Flow Repository modules;
- Rule Based Engine (RBE) is represented by combination of PDP used for individual policies evaluation and FCE that control multiple policies evaluation or other sequence of policy evaluation for the complex resource.

Technically, two specified GAAA profiles use the same set of functional components but have different configuration of components related to security context (including key, trust relations, external call-outs configuration), internal components interaction and also required ASM functionality. The major idea behind defining two actually intersecting profiles is too simplify design and improve manageability and configuration during deployment.

As resulted from the practical implementation in the CNL project, GAAA-RBAC is extended with two additional features that are often missing in available access control implementations: authorisation session revocation and configuration management interface to configure multiple trust domains for interacting services.

When providing access control during the long-running or multistage experiment, the security context (e.g., policies, team members, roles) may change. Such changes may be controlled in the experiment workflow and fed into access control system via advanced configuration management interface to GAAAPI modules.

Separation of the flow processing and individual resources' policy evaluation in service provisioning

scenario allows separating business related part of the provisioning process and policies applied to individual services or resources that are rather static and managed by service providers. Provider of a complex service can apply its own provisioning model that may have different sequence of individual policies evaluation and other conditions related to the overall provisioning process.

With the workflow and policy separation, three levels of the service request evaluation against the provisioning or individual policy can be defined:

- one step (or instant) request evaluation by Triage that simply checks (instant) request matching against provided AuthZ ticket/token or instant push-policy;
- resource/service policy evaluation by the PDP that does request evaluation according to the policy that itself describes a sequence of provided attributes/information evaluation, e.g. in XACML evaluation sequence includes first target (subject, resource, action) matching, next rules evaluation and finally rules combination to make overall policy based decision;
- complex request evaluation that requires multiple policies evaluation in the sequence described by provider or request specific (business) flow; in this case the FCE take care about driving the evaluation and provisioning process.

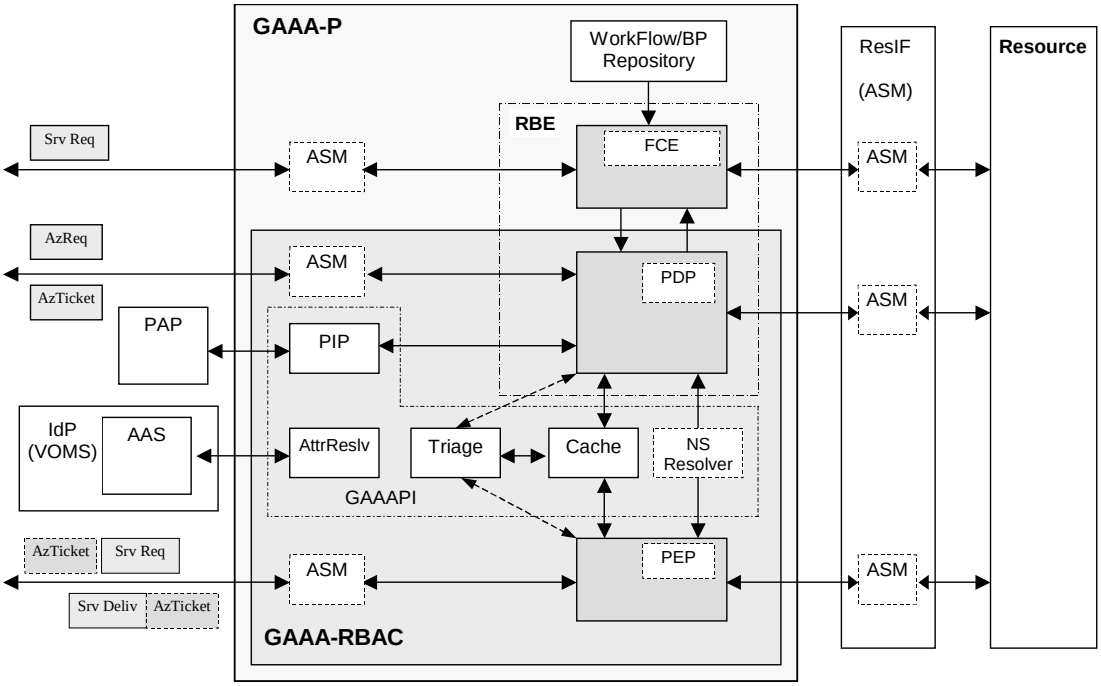

Figure 3. GAAA-RBAC and GAAA-P profiles and main functional components

Outsourcing combination of individual policies evaluation to upper layer FCE function will simplify multiple policies management in sense that there will not be a need for the overall policy validation to avoid possible conflicts and attributes conversion.

4.2. Integration with the GT4 and gLite Authorisation Frameworks

GT4 Authorisation Frameworks [14] is a component of the widely used Grid middleware that provides general and specific functionality to control access to Grid applications and resources using access control policies in a specific for Grid formats like Access Control Lists (ACL), gridmap file, identity or host based, and also providing external policy evaluation callouts using OGSA Authorisation PortType [15] that uses SAML messaging format. Simple XACML based PDP is provided also.

In current implementation the gLite security middleware [16] uses the GT4 Authorisation Framework with some specific extension for different Grid services.

GAAA_tk is being developed to be compatible with both GT4 and gLite toolkits but with the priority to

provide necessary functionality for collaborative applications that are not yet fully based on Grid or Web services. With gradual migration to Grid services and wider use of the GT4 middleware, integration with the GT4 Authorisation Framework can be done in three ways: (1) using GT4 WS/messaging firmware to provide WS-based access to GAAA_tk authorisation service to allow easy GAAA_tk integration into different applications; (2) adding GAAA AuthZ callouts to GT4 AuthZ framework; (3) integrating GAAA AuthZ PDP/GAAAPI into GT4 AuthZ framework as one of internal PDP's.

GAAA_tk based applications can benefit from using a number of features specific to GT4/OGSA Security Infrastructure that include support for different types of secure credentials, in particular, X.509 Proxy and Attribute Certificates, VOMS credentials, and support for WS-Trust based secure communication. On other hand, GAAA_tk can add to the GT4 Authorisation Framework such functionality as authorisation session management, authorisation tickets and tokens handling, complex XACML policies evaluation, flexible trust domains and request semantics configurations and management.

5. USING XACML AND SAML FOR POLICY EXPRESSION AND SECURITY ASSERTIONS

XACML (eXtensible Access Control Markup Language) defines rich policy format for the generic RBAC and simple Request/Response messages format for PEP-PDP communication [17]. XACML policy is defined for the so-called target triad "Subject-Resource-Action" which can also be completed with the Environment element to add additional context to instant policy evaluation.

XACML policy format can also specify actions that must be taken on positive or negative PDP decision in the form of Obligation element, which is an optional element of the Policy. This functionality is important for possible integration of the access control system with the logging or auditing facilities.

Decision request sent in a Request message provides context for the policy-based decision. The policy applicable to a particular decision request may be composed of a number of individual rules or policies. Few policies may be combined to form a single policy applicable to the request. XACML specifies a number of policy and rule combination algorithms. The Response message may contain multiple Result elements, however related to individual Resources.

New XACML specification 2.0 defines three special profiles that can extend XACML functionality in evaluation of complex requests what is important for fine-grained access control to complex resources/instruments in GCE:

The XACML RBAC profile [18] describes how to built Policies requiring multiple Subjects and roles combination to access a resource and perform an action. Multiple Subject elements in XACML allow flexibility when implementing hierarchical RBAC model for such cases when some actions require superior subject/role approval to perform a specific action. For example, one Subject might represent the human user that initiated the application from which the request was issued; another Subject might represent the application's executable code responsible for creating the request; another Subject might represent the machine on which the application was executing; and another Subject might represent the entity that is to be the recipient of the Resource. In such a way, RBAC profile can significantly simplify rights delegation inside the group of collaborating entities/subjects which normally requires complex credentials management.

The XACML hierarchical resource profile [19] specifies how XACML can provide access control for a Resource that is organized as a hierarchy, which examples are the file systems, data repository, XML documents, or organizational resources.

The XACML Multiple Resources profile [20] allows for complex request to multiple resources having the same request context, in this case the single Resource element will contain composition of all resources to be evaluated together. Request processing may involve decomposing the one complex Resource Request into many individual Resource Requests before evaluation by the PDP.

Although XACML defines Request/Response messages format, it doesn't provide any suggestions about using one or another transport container or protocol and security mechanisms to protect messages security, i.e. authenticity, integrity and confidentiality, and other features important for security assertions including binding authority to the decision or applying validity restrictions to the assertion. However, all required functionality is available in another XML based format SAML (Security Assertion Mark-up Language) that can be used for security assertions expression and exchange [18]. It is logical and widely used solution to combine XACML policy based decision making and SAML for security assertions expression and communication with Authentication, Authorisation and Attribute services.

Practical use of XACML and SAML will require definition of own assertion types and attribute namespaces for all assertion and policy components. In discussed above access control model, SAML can be used as a security assertions format in particular for AuthzTicket expression for performance optimisation. AuthzTicket can be expressed as a native SAML Authorization Assertion [21] or as a XACMLAuthzDecisionStatement [22] that simplifies integration with XACML. Current GAAAPI implementation supports both SAML-based and proprietary XML-based AuthzTicket formats.

The AuthzTicket is generated as the result of a positive PDP decision. It contains the decision and all necessary information to identify the requested service. When presented to the PEP, its validity can be verified and in the case of a positive result, access will be granted without requesting a new PDP decision. Such a specific functionality is provided in the GAAA_tk with the Triage module (see section 4).

Other required functionality such as session management and validation of security tokens used as attributes in authorisation request can be supported by GAAAPI/PIP functionality provided by GAAA_tk.

6. USING VO FOR DYNAMIC SECURITY ASSOCIATIONS MANAGEMENT

In Grid applications and projects, VO is used as a framework for establishing project related resource sharing and user attributes management [2, 23]. Access to these shared distributed resources is provided based on the VO membership and other VO-related attributes like groups and roles. This section attempts to review current VO concept and provide suggestions how the VO as an abstract concept and as a practical implementation can be used for more general federated and/or dynamic trust management in GCE.

6.1. VO and Dynamic Security Associations

When considering the VO as a virtual entity for managing security context (providing user attributes) for dynamic processes and associations we can build the following list of different types of security associations relevant to typical GCE use cases and their dynamics (or lifetime characteristics):

- **Session** – establishes security context in the form of session key that can be a security token or simple UID bound to session initiator's secure credential. Session may associate users, resources and actions/processes.
- **Experiment/workflow** – this may be more long-lived association and include few sessions. Experiment or workflow is created for the specific task generally defined by the contract either to perform some work or deliver product. They may need to associate distributed collection of users and resources for longer time required to deliver a final product or service. Security context may change during workflow execution or Experiment lifetime. Experiment description, as discussed in the section 2, may contain both user and resource lists and also provide trust anchor(s) (TA) and security policy reference.
- **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 fulfilment. This is actually the area of currently existing VO based associations widely used in Grid.
- **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 example are the Shibboleth-based federations and which acceptance by the Grid community is expected with the development of the special GridShib profile [24, 25].

Relevant to the GCE, the Experiment/workflow and project oriented 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.

VO attribute or membership service is used for trusted attribute 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 [23].

6.2. VO Management Framework

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.

VO can be established according to a well-defined procedure and based on a framework agreement between

member organisations to commit their resources to the VO and adhere common policy that may be simple enough but not to contradict to the local security policies at member institutions.

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. By establishing and managing own federated/associated security domain, VO helps to overcome limitations of the member enterprise local security policies/boundaries and enable cooperation without changing local security policies and user management, including providing firewall bypass for registered VOs.

Major VO membership management tool used as a standard-de-facto in current Grid applications is the VO Membership Service (VOMS) [26]. VOMS provides VO-defined attribute for authorisation and also supports user registration procedure with the VOMS Admin server automated workflow. When considered for support of dynamic security associations, VOMS can be adopted to wide range of dynamics and can be easily integrated with the experiment-centric or customer driven security model. In GCE/CNL, VO can be created based on signed collaboration framework agreement (e.g., Virtual Laboratory) or experiment agreement and used for both providing security context (attributes and trust anchors) for all activities related to a particular experiment, and for inter-organisational resource advertising and sharing.

7. CONCLUSION AND SUMMARY

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 service provisioning and collaborative resource sharing conducted by the System and Network Engineering (SNE) 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.

Adding workflow management as a component of integrated security model/infrastructure allows to separate security services/functionality related to actual/traditional security middleware and those related to business logic, at the same time providing their tight integration. Thus, such approach allows to simply manage security context of the authorisation service, e.g. access control policies, attributes and credential authorities by feeding it into the contributing organisations and services without need to harmonise them globally for the whole collaborative infrastructure.

The CNL access control architecture is based on the proposed Experiment-centric security model that is extended with the workflow management capability what allows to separate semantic and executive components in experiment and access control management and combine them at the process/flow decision points. This will allows to simply provide security context to authorisation/policy decision points based on current experiment status and involved parties and domains, in particular, combine general and local policies and security context. Flow management functionality can also resolve and handle possible conflicts between local and experiment wide security policies.

Proposed implementation is based on the special GAAA-RBAC profile of the GAAA Toolkit and provides all necessary functionality to evaluate complex service requests that may require multiple policies and attributes evaluation. The AuthZ tickets and tokens handling functionality allows for performance optimisation and supports authorisation session management. GAAA-RBAC uses XACML for policy expression including special profiles for complex and hierarchical resource profiles and SAML for assertions expression and communications with external security services providers. GAAA-RBAC is easily extended with the flow management functionality to handle complex context dependent authorisation requests (for service provisioning) that require conditional and multi-step evaluation.

Another important topic discussed in this paper is related to the use of the Virtual Organisation concept for managing dynamic security associations in collaborative applications and for complex resource provisioning in general. The paper identifies basic requirements to VO management functionality. The major goal of the proposed analysis is to promote the VO, as one of key concept in Grid, to industry and bridge between traditional Identity and attribute management technologies and those used in VO.

The authors believe that the proposed access control architecture for Grid based collaborative applications and related technical solutions will be useful to wider community that deal with the development of middleware for dynamic collaborative applications that may benefit from using Grid-based service-oriented security infrastructure for management of resources and services.

8. REFERENCES

[1] "Web Services Architecture". W3C Working Draft 8 August 2003. - http://www.w3.org/TR/ws-arch/

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

[3] 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.

[4] Demchenko, Y., L. Gommans, C. de Laat, B.Oudenaarde, A. Tokmakoff, M. Snijders, R. Buuren, "Security Architecture for Open Collaborative Environment," - European Grid Conference, EGC 2005, Amsterdam, The Netherlands, February 14-16, 2005, Proceedings. Series: Lecture Notes in Computer Science, Volume 3470, 2005.

[5] Zhiming Zhao et al, "Including the State of art scientific workflow management systems in an e-Science environment", available at http://staff.science.uva.nl/ ~zhiming/project/vl-e/ZhaoZ-UvA-e-Science-workflow-paper.pdf

[6] OASIS Web Services Business Process Execution Language (WSBPEL) TC - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel

[7] Business Process Execution Language for Web Services version 1.1, July 30, 2002. - http://www-128.ibm.com/developerworks/library/specification/ws-bpel/

[8] Andrieux, A. et al, "Web Services Agreement Specification (WS-Agreement)," August 2004, available from https://forge.gridforum.org/projects/graap-wg/document/WS-AgreementSpecification/

[9] Grid Distributed Resource Management Application API (DRMAA), available from https://forge.gridforum.org/projects/drmaa-wg

[10] Information Technology - Role Based Access Control, Document Number: ANSI/INCITS 359-2004, InterNational Committee for Information Technology Standards, 3 February 2004, 56 p.

[11] Generic Authorization Authentication and Accounting. - http://www.science.uva.nl/research/air/ projects/aaa/

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

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

[14] GT 4.0: Security: Authorization Framework. - http://www.globus.org/toolkit/docs/4.0/security/authzframe/

[15] Welsh, V. et al, "Use of SAML for OGSI Authorization", GGF Darft, August 15, 2005, available from https://forge.gridforum.org/projects/ogsa-authz

[16] gLite Security Subsystem. - http://glite.web.cern.ch/glite/security/

[17] Godik, S. et al, "eXtensible Access Control Markup Language (XACML) Version 2.0", OASIS Working Draft 04, 6 December 2004, available from http://docs.oasis-open.org/xacml/access_control-xacml-2_0-core-spec-cd-04.pdf

[18] Core and Hierarchical Role Based Access Control (RBAC) profile of XACML, Version 2.0. Committee Draft 01, 11 November 2004 - http://docs.oasis-open.org/xacml/access_control-xacml-2.0-rbac_profile1-spec-cd-01.pdf

[19] Hierarchical Resource profile of XACML. Committee Draft 01, 11 November 2004 - http://docs.oasis-open.org/xacml/access_control-xacml-2.0-hier_profile-spec-cd-01.pdf

[20] Multiple Resource profile of XACML. Committee Draft 01, 11 November 2004 - http://docs.oasis-open.org/xacml/access_control-xacml-2.0-mult_profile-spec-cd-01.pdf

[21] Cantor, S. et al, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," Committee Draft 04, 14 January 2005, available from http://www.oasis-open.org/committees/download.php/10627/sstc-saml-core-2.0-cd-03.pdf

[22] Anderson, A. et al, "SAML 2.0 profile of XACML," OASIS Committee Draft 02, 11 November 2004, available from http://docs.oasis-open.org/xacml/access_control-xacml-2.0-saml_profile-spec-cd-02.pdf

[23] Demchenko, Y., et al., "VO-based Dynamic Security Associations in Collaborative Grid Environment". – This issue, Pages ??-??.

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

[25] GridShib - A Policy Controlled Attribute Framework. - http://grid.ncsa.uiuc.edu/GridShib/

[26] Virtual Organisation Membership Service (VOMS) – http://infnforge.can.infn.it/voms/