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 design and development of a flexible, customer-driven, security infrastructure for Grid-based Collaborative Environments. The paper proposes further development of the access control model built around a service or resource provisioning agreement (e.g., an 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 lifetime of an experiment. The paper analyses the required functionality and suggests extensions to the generic AAA Authorisation framework in order to support complex collaboration scenarios in dynamic virtualised environments. The paper provides implementation details on the use of XACML for fine-grained access control policy definition for complex resources and team-based role 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 association management. The proposed technical solutions are intended to be compatible and interoperable with the current implementation of the Grid security middleware in the Globus Toolkit and gLite. The paper is based on experiences gained from 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 support of its normal operation and for the processing of experiment results. It also requires a corresponding infrastructure that is created for the purpose of running experiments 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) agreements and terminated once the experiment has been completed.

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

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

In a GCE, security services and infrastructure play an important role in providing reliable and secure resources/instrument access and service delivery. This paper describes our experiences when developing a flexible, customer-driven, security infrastructure for a dynamic GCE. It proposes further development of the Job-centric security model built around the service or resource provisioning agreement (e.g., an experiment or a project) proposed in [3] and being developed in the framework of the Collaboratory.nl[4] project (CNL). Although our proposed solution can provide a general, experiment-defined security context for all security services operation, there is no possibility to change this context during an experiment's lifetime.

The paper looks into further improvement and automation of the management of experiment components and supporting services during the experiment's lifetime. In particular, we discuss the use of workflow management technologies for dynamic security context management and for an instant access control policy definition.

The paper is organized as follows. Section 2 provides brief information about recent developments in the CNL project, discusses experiences with the implementation of the Job-centric security model, and provides motivation for its extension and use of workflow management technology. Section 3 explains how the 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 resource control and for team-based access rights delegation.

Section 5 provides suggestions on how the Virtual Organisation (VO) concept can be used to create dynamic security associations of users and resources, based on the collaboration or experiment agreement. This should allow establishment of inter-organisational trust relations and provide VO members with access to internal resources without needing to change their organisational security policy.

The proposed approach and solutions respond to both common and domain-specific requirements of 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]. The paper [3] provided an introduction into the proposed Job-centric security model and discussed important issues such as performance and optimisation issues, trust management in a distributed access control infrastructure, multiple policy evaluation and combination of multiple authorisation decisions.

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

Continuing with the general design approach of using Grid and Web Services platforms, 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 require 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 hand-configuring and managing user accounts and instruments. This resulted in slow adaptation of the working space, a high administrative overhead and overly 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.

The 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 of some security services (including access control policies) at different stages in the experiment. This means that workflow management framework and tools for an experiment-centric, customer-driven GCE should also allow management of the security context and callouts to security services.

Recently, technologies and tools for managing scientific workflow and business processes have attracted great interest throughout the e-Science community and in the business world. The paper [4] provides a comprehensive overview and analysis of available Scientific Workflow Management Systems (SWMS) and their use for automation of experiments. Most SWMS have been developed and used in the framework of different e-Science research projects and are often oriented toward specific scientific research areas.

With the development of Web Services, industry has focused on developing business process management and execution frameworks for Web Services. Workflow description standardisation is currently ongoing in the framework of the OASIS Web Services Business Process Execution Language (WSBPEL) TC. This effort is based on the earlier proposed BPEL4WS standard that was developed by leading industry players such as IBM, Microsoft, Oracle, and others [5, 6]. Currently, available BPEL design and execution tools can simplify a major part of 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 basis 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 the experiment and manage the dynamic security context. In particular, the VO membership service needs to manage users and their roles, policy (or a set of policies), and a 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 [7] to have potential compatibility with the Grid Distributed Resource Management Application framework (DRMAA) [8]. Each experiment description exists in the form of an XML document and can be used as the scope for developing a workflow with standard workflow design tools.

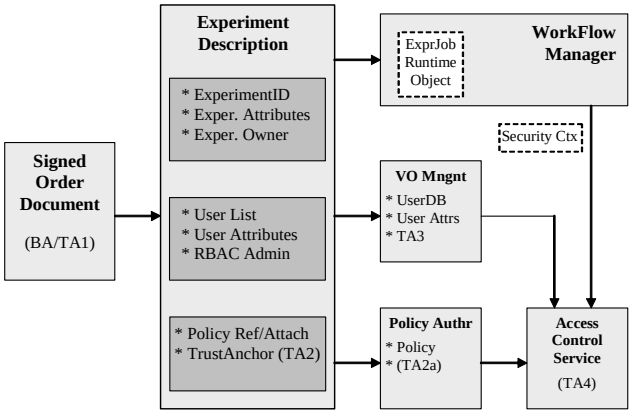

Figure 1. Workflow and security context in GCE

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

The experiment-centric and workflow-driven security model is logically integrated with other stages and components of the collaborative (virtual) organisation managing the experiment stages. A VO can provide a good platform/solution for managing dynamically established trust relations between member organisations that are in the process of performing a specific experiment.

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

Fine-grained access control in typically interactive services in a GCE can be achieved using the Role-Based Access Control (RBAC) authorisation model, which generally consists of major functional components that include: Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Authority Point (PAP) [9]. In RBAC,

user/requestor access rights are defined by roles in a form of user attributes and a 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. A Resource or Service is protected by site access control system that relies 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 that they can evaluated by calling back to the 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.

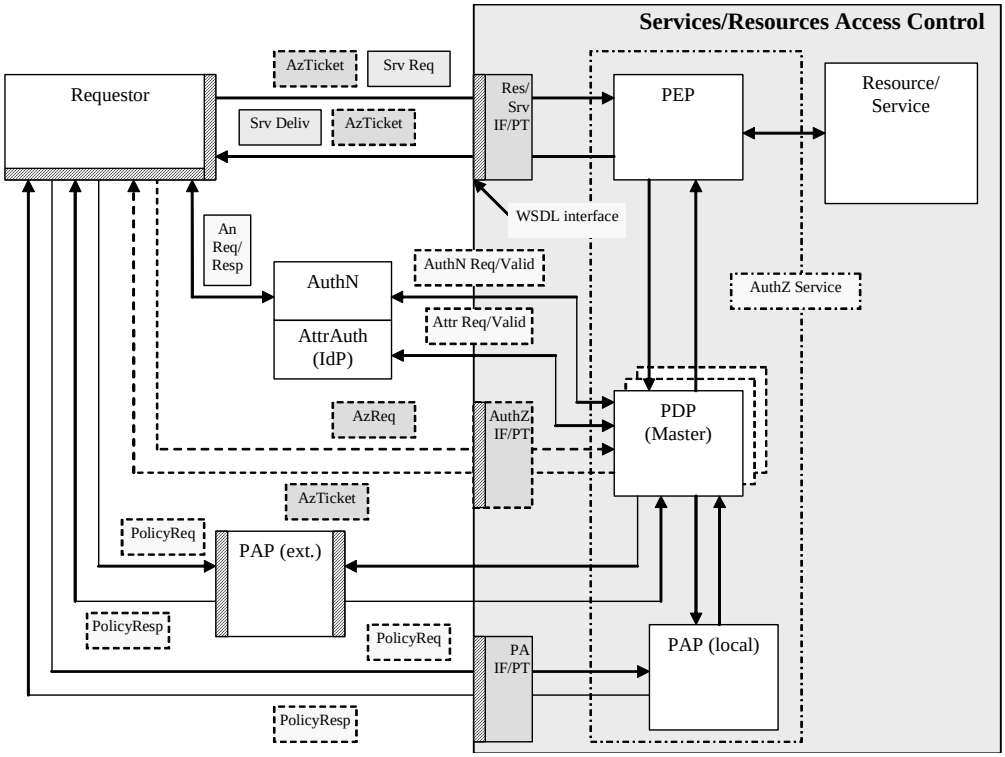

Figure 2. Main interacting components involved in access control in a typical Grid-based collaborative application

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

A typical access control use-case may require a combination of multiple policies and also 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 stage of the experiment.

The paper [3] provides an analysis and suggestions on how an instant service request evaluation can be done against multiple policies (by combining policies or combining the PDP and the PEP), however this approach requires additional processing in case of complex resource provisioning and stateful request 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 management of multiple policies.

4. EXTENDING GAAA AUTHORISATION FRAMEWORK FOR DYNAMIC COLLABORATIVE APPLICATIONS

The above-described 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 [10]. GAAA_tk provides basic functionality for the Generic Authentication, Authorisation and Accounting (GAAA) Authorisation framework described in [11, 12]. It features two basic profiles: an RBAC profile for collaborative applications specifically targeted at fine-grained team-oriented access control to shared resources, and a GAAA-P profile for complex resource/service provisioning in a multi-domain, distributed, and service-oriented environment.

To support dynamic security context changes, the GAAA_tk provides an advanced configuration management capability, based on the generic AuthZ service operational model. Adding workflow processing functionality to the GAAA-P profile (in combination with a rich policy evaluation capability in the GAAA-RBAC profile) allows for complex multi-domain policy evaluation and execution of complex provisioning algorithms.

4.1. GAAA-RBAC Implementation with the GAAA Toolkit

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

- GAAAPI provides all the necessary functionality for communication between a PEP and a PDP. It also provides a security context for evaluation of service requests versus the service (access) policy, which includes:
  - A namespace resolver to define/resolve what policy and what attributes should be used for the request evaluation;
  - Triage and Cache functionality that provides an initial evaluation of the request, including the validity of the provided credentials. This functionality is used for handling AuthZ tickets/tokens and also for AuthZ session management by evaluating service requests versus the provided AuthZ ticket/token claims;
  - An 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 the Identity Provider service (IdP);
- The GAAA-RBAC subsystem provides the GAAA-RBAC profile functionality and comprises of a PEP, a PDP and the GAAAPI, along with related Application Specific Modules (ASM);
- The GAAA-P subsystem includes the GAAA-RBAC subsystem used for general policy evaluation and adds flow control with the Flow Control Engine (FCE) and Flow Repository modules;
- The Rule-Based Engine (RBE) is represented by a combination of the PDP, which is used for individual policy evaluation, and the FCE, which controls multi-policy evaluations or other sequences of policy evaluation for a complex resource.

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

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

When providing access control during a long-running or multi-stage experiment, the security context (e.g., the

policies, team members and/or roles) may change. Such changes may be controlled in the experiment workflow and fed into access control system via an advanced configuration management interface to GAAAPI modules.

Separation of flow processing from individual resources' policy evaluation in service provisioning scenarios allows separation of the business-related aspects of service provisioning from the policies that are applied to individual services or resources (which are rather static and managed by service providers). The provider of a complex service can apply its own provisioning model that may have a different sequence of individual policy evaluations and other conditions related to the overall provisioning process.

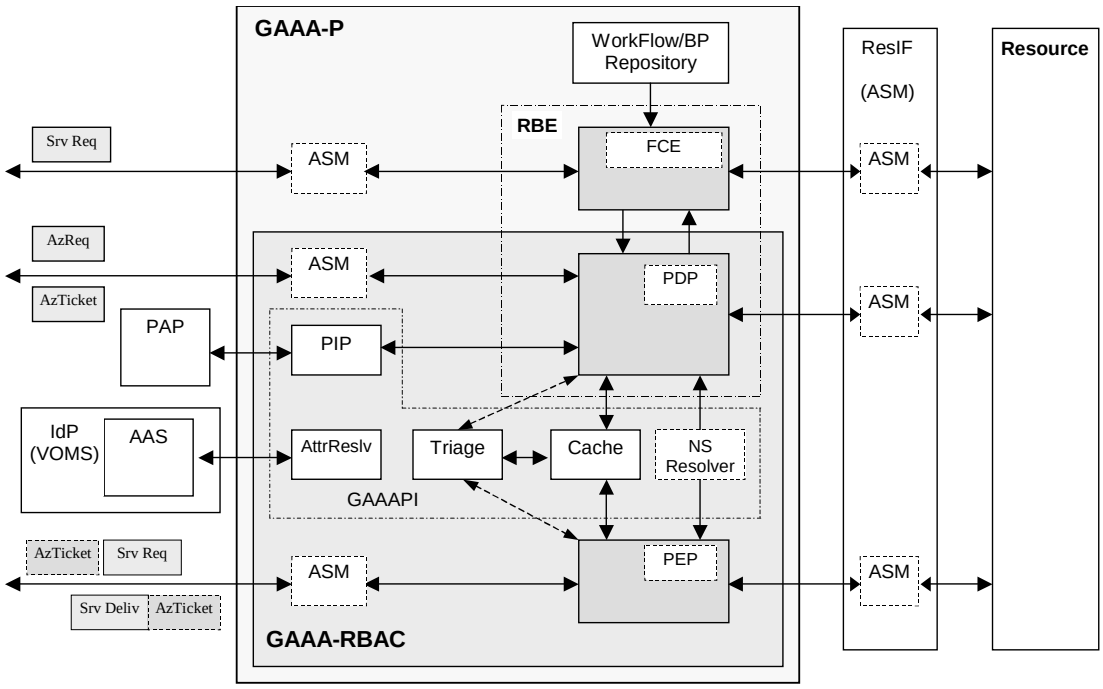

Figure 3. GAAA-RBAC and GAAA-P profiles and main functional components

With the separation of workflow and policy, 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 the provided AuthZ ticket/token or instant push-policy;
- resource/service policy evaluation by the PDP that performs request evaluation according to the policy that describes a sequence of provided attributes/information evaluation, e.g. in XACML evaluation a sequence includes firstly the target (subject, resource, action) matching, next the evaluation rules and finally the combination rules to make an overall policy based decision;
- complex request evaluation that requires evaluation of multiple policies in the sequence described by the provider or request-specific (business) flow. In this case the FCE takes drives the evaluation and provisioning process.

Outsourcing a combination of individual policy evaluations to the upper layer FCE function will simplify multiple policy management in the sense that there will not be a need to perform an overall policy validation step to avoid possible conflicts and attribute conversions.

4.2. Integration with the GT4 and gLite Authorisation Frameworks

GT4 Authorisation Frameworks [13] 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 Grid-specific formats, such as Access Control Lists (ACLs), gridmap file, identity or host based, and also providing external policy evaluation callouts using OGSA Authorisation PortType [14] that uses SAML as a messaging format. A simple XACML-based PDP is also provided.

In the current implementation the gLite security middleware [15], the GT4 Authorisation Framework is used, with some specific extensions for different Grid services.

GAAA_tk is being developed to be compatible with both the GT4 and gLite toolkits, but with a priority goal being to provide the 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 performed in three ways:

(1) using GT4 WS/messaging firmware to provide WS-based access to the GAAA_tk authorisation service, thereby allowing easy GAAA_tk integration into different applications;

(2) adding GAAA AuthZ callouts to the GT4 AuthZ framework;

(3) integrating GAAA AuthZ PDP/GAAAPI into the GT4 AuthZ framework as one of its internal PDP's.

GAAA_tk-based applications can benefit from using a number of features that are specific to GT4/OGSA Security Infrastructure that includes 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 the other hand, GAAA_tk can add to the GT4 Authorisation Framework functionality such as authorisation session management, handling of authorisation tickets and tokens, complex XACML policy evaluation, flexible trust domains and request semantics configuration and management.

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

eXtensible Access Control Markup Language (XACML) defines a rich policy format for the generic RBAC and also for the simple Request/Response messages format used for PEP-PDP communication [16]. A 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.

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

A 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 that is applicable to the request. XACML specifies a number of policy and rule combination algorithms. The Response message may contain multiple Result elements, which are related to individual Resources.

The three special profiles extend XACML functionality, which is important for fine-grained access control to complex resources/instruments in GCE:

The XACML RBAC profile [17] describes how to build Policies that require multiple Subjects and roles combination to access a resource and perform an action. Multiple Subject elements in XACML allow flexibility when implementing hierarchical RBAC models in 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 [18] specifies how XACML can provide access control for a Resource that is organized as a hierarchy. Examples include file systems, data repositories, XML documents and organizational resources.

The XACML Multiple Resources profile [19] allows for complex requests to multiple resources that have the same request context. In this case, the single Resource element will contain a composition of the all resources to be evaluated together. Request processing may involve decomposing the single complex Resource Request into numerous individual Resource Requests before evaluation by the PDP.

Although XACML defines a Request/Response messaging format, it doesn't provide any suggestion regarding one or another transport container or protocol to use, security mechanisms to protect message security. This includes authenticity, integrity and confidentiality, and other features that are 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 [20]. 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 the definition of own assertion types and attribute namespaces for all assertion and policy components. As discussed above, SAML can be used as a security assertion format, in particular for AuthzTicket expression for performance optimisation. AuthzTicket can be expressed as a native SAML Authorization Assertion or as a XACMLAuthzDecisionStatement [21] which simplifies integration with XACML. The current GAAAPI implementation supports both SAML-based and proprietary XML-based AuthzTicket formats.

An 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, 22]. 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 present the current VO concept and provide suggestions on 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 contexts (providing user attributes) for dynamic processes and associations, we can build the following list of different types of security associations that are relevant to typical GCE use cases and their dynamics (or lifetime characteristics):

- **Session** – establishes security context in the form of a session key that can be a security token or simple UID bound to the session initiator's secure credential. A session may associate users, resources and actions/processes.
- **Experiment/workflow** – this may be a more long-lived association and include a few sessions. An experiment or workflow is created for the specific task (generally defined by the contract) either to perform some work or deliver a product. Experiments may need to associate a distributed collection of users and resources for longer time, as required to deliver a final product or service. The security context may change during workflow execution or Experiment lifetime. An experiment description (as discussed in the section 2), may contain user and resource lists and also provide trust anchor(s) (TA) and a security policy reference.
- **Project or mission oriented cooperation** – this type of association is established for long term 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 a criteria of mission fulfilment. This is actually the area of currently existing VO-based associations that are 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. An example id this is Shibboleth-based federations, whose acceptance by the Grid community is expected with the development of the special GridShib profile [23, 24].

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.

6.2. VO Management Framework

A 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.

A 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 also to adhere to a common policy that may be simple but not contradictory to the local security policies at member institutions. A VO attribute or membership service provides trusted attribute brokering between member organisations when requesting resources or services from the VO members or their associates.

The VO establishes its 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 the VO security domain, but also requires coordination with the security policies in member organisations. By establishing and managing its own federated/associated security domain, a VO helps to overcome the limitations of the member enterprises' local security policies/boundaries and enables cooperation without changing of local security policies and user management (including providing firewall access for registered VOs).

A major VO membership management tool used as a de-facto-standard in current Grid applications is the VO Membership Service (VOMS) [25]. VOMS provides VO-defined attributes for authorisation and also a supports user registration procedure with the VOMS Admin server's automated workflow. When considered for its support of dynamic security associations, VOMS can be adapted to a wide range of dynamics and can be easily integrated with the experiment-centric or customer-driven security model. In GCE/CNL, a VO can be created based on a signed collaboration framework agreement (e.g., Virtual Laboratory) or an experiment agreement, and used for both providing a 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 and its application to user-controlled service provisioning and collaborative resource sharing. This work is being conducted by the System and Network Engineering (SNE) Group in the framework of different EU and Dutch nationally-funded projects including EGEE, NextGRID, Collaboratory.nl, and GigaPort Research on Network. All of these projects deal with the development, deployment or use of Grid technologies and middleware infrastructure platforms whilst also providing a broad scope of different use cases for both the Grid and the GAAA Framework.

Adding workflow management as a component of an integrated security model/infrastructure allows separation of security services/functionality related to actual/traditional security middleware from those related to business logic, whilst at the same time providing their tight integration. Thus, such an approach allows simple management of the 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 a 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 has been extended with a workflow management capability. It allows separation of semantic and executive components in an experiment from access control management and combines them at the process/flow decision points. The workflow management system can provide a changing security context to authorisation/policy decision points based on the current experiment status, and the involved parties/domains. Flow management functionality can also resolve and handle possible conflicts between local and experiment-wide security policies.

The proposed implementation is based on the special GAAA-RBAC profile of the GAAA Toolkit and provides all of the necessary functionality to evaluate complex service requests that may require multiple policies and attributes evaluation. The AuthZ ticket and token 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 expression of assertions and communication with external security service providers. GAAA-RBAC is easily extended with 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 for VO management functionality. The major goal of the proposed analysis is to promote the VO to industry as a key concept in Grid that can bridge the gap between traditional identity and attribute management technologies and more advanced techniques used in VO.

The authors believe that the proposed access control architecture for Grid based collaborative applications and

related technical solutions will also be useful to the wider community that deals with the development of middleware for dynamic collaborative applications which can benefit from using a 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] Foster, I. et al, "The Open Grid Services Architecture, Version 1.0", Global Grid Forum, 29 January 2005, available from http://www.gridforum.org/documents/GFD.30.pdf

[3] Demchenko, Y., L. Gommans, C. de Laat, B. Oudenaarde, A. Tokmakoff, M. Snijders, "Job-centric Security model for Open Collaborative Environment," The 2005 International Symposium on Collaborative Technologies and Systems, Saint Louis, USA, May 15-19, 2005, Proceedings. IEEE Computer Society, ISBN: 0-7695-2387-0, pp. 69-77.

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

[5] "Web Services Business Process Execution Language. Version 2.0", OASIS Committee Draft, 21 December 2005, available from http://www.oasis-open.org/committees/download.php/16024/wsbpel-specification-draft-Dec-22-2005.htm

[6] "Business Process Execution Language for Web Services version 1.1", Updated February 1, 2005. available from http://www-128.ibm.com/developerworks/library/specification/ws-bpel/

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

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

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

[10] Generic Authorization Authentication and Accounting. [Online]. Available: http://www.science.uva.nl/research/air/projects/aaa/

[11] 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

[12] 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

[13] GT 4.0: Security: Authorization Framework. [Online]. Available: http://www.globus.org/toolkit/docs/4.0/security/authzframe/

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

[15] gLite Security Subsystem. [Online]. Available: http://glite.web.cern.ch/glite/security/

[16] 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

[17] "Core and hierarchical role based access control (RBAC) profile of XACML v2.0", OASIS Standard, 1 February 2005, available from http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf

[18] "Hierarchical resource profile of XACML 2.0", OASIS Standard, 1 February 2005, available from http://docs.oasis-open.org/xacml/access_control-xacml-2.0-hier_profile-spec-cd-01.pdf

[19] "Multiple resource profile of XACML 2.0", OASIS Standard, 1 February 2005, available from http://docs.oasis-open.org/xacml/access_control-xacml-2.0-mult_profile-spec-cd-01.pdf

[20] 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

[21] 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

[22] Demchenko, Y., et al., "VO-based Dynamic Security Associations in Collaborative Grid Environment," The 2006 International Symposium on Collaborative Technologies and Systems, Las Vegas, NV, USA, May 14-18, 2006, Accepted.

[23] Shibboleth Project. [Online]. Available: http://shibboleth.internet2.edu/

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

[25] Virtual Organisation Membership Service (VOMS). [Online]. Available: http://infnforge.can.infn.it/voms/