Using Workflow for Dynamic Security Context Management in Grid-based Applications

Yuri Demchenko[#1], Leon Gommans[#2], Cees de Laat[#3], Arie Taal[#4], Alfred Wan[#5], Olle Mulmo[*6]

[#]*System and Network Engineering Group, University of Amsterdam*
Kruislaan 403, 1098SJ, Amsterdam, The Netherlands
[1]demch@science.uva.nl, [3]lgommans@science.uva.nl
[3]delaat@science.uva.nl, [4]taal@science.uva.nl
[5]wan@science.uva.nl

[*]*Center for Parallel Computers, Kungliga Tekniska högskola*
SE-100 44 Stockholm, Sweden
[6]mulmo@pdc.kth.se

***Abstract*— This paper presents ongoing research and current results on the development of flexible access control infrastructures for complex resource provisioning in Grid-based collaborative applications and on-demand network services provisioning. We investigate the use of workflow concepts for the required orchestration of multiple Grid resources and/or services across multiple administrative and security domains. In particular, workflow execution and management tools can be used to track security context changes that are dependent on the application domain, execution stage defined policies, or user and/or service attributes. The paper discusses what specific functionality should be added to Grid-oriented authorization frameworks to handle such dynamic service-related security contexts. As an example, the paper explains how such functionality can be achieved in the GAAA Authorization framework and GAAA toolkit. Suggestions are given about integration with the Globus Toolkit's Authorization Framework. Additionally, the paper analyses what possibilities of expressing and handling dynamic security contexts are available in XACML and SAML, and how the VO concept can be used for managing dynamic security associations of users and resources. The paper is based on experiences gained from major Grid based and Grid oriented projects such as EGEE, NextGrid, Collaboratory.nl and GigaPort Research on Network.**

I. INTRODUCTION

With wider use and deployment of the Grid and Web Services there is increasing industry demand for dynamic, customer-driven service and resource provisioning. In this case, the Grid security infrastructure should allow for a dynamic binding of an invoked Grid service and its security policy, and, in particular, be dependent on the task execution context. While the Open Grid Services Architecture (OGSA) [1] shows great promise at providing an architectural framework for dynamic Grid services, a practical implementation requires a more detailed definition on the operational aspects.

Lately, Grid middleware has been developed 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 primary focused on computational resources and tasks management. At the same time many collaborative and business-oriented applications require more complex and interactive Grid services management scenarios [2].

Grid middleware provides a common communication/messaging infrastructure for all resources and services exposed as Grid services, and also allows for a uniform security configuration at the service container or messaging level. This significantly simplifies development of Grid-based applications and allows developers to focus on application-level logic.

The topic of this paper is developing principles and providing suggestions how the access control infrastructure can be built to support a dynamically changing security context and yet be capable of providing consistent security. Currently, this issue is not addressed in existing security middleware implementation. All major components of the security context, such as trust relations, attributes semantics, and access control policies typically need to be statically configured before service deployment. Making them dynamically configurable and manageable during the service operation is considered in this paper as an approach to designing context-aware access control services for dynamic Grid applications.

This work is based on two use cases that define basic functionality in a flexible and dynamic access control infrastructure: Optical Light Path Provisioning (OLPP) [3] and Grid-based Collaborative Environments (GCE) [4].

Approaches and technical solutions proposed in this paper are based on an extended gap analysis undertaken in the framework of the SURFnet GigaPort Research on Network (GigaPort-RoN) [4] project to identify general and specific requirements to access control infrastructure for on-demand network services provisioning, in particular, OLPP [5].

[1] http://public.eu-egee.org/

[2] http://www.opensciencegrid.org
[3] http://www.globus.org/
[4] http://ron.gigaport.nl/

Significant improvement in the performance and manageability of the service and resource provisioning can be achieved with the use of workflow management technologies and tools. Additionally, workflow can add business logic to the provisioning process and automate the user-provider relationship, e.g. through the negotiation and establishment of Service Level Agreements (SLA) at run-time. In this paper, we investigate how the workflow concept can additionally be used for managing a dynamic security context, with a primary focus on access control decisions.

The paper is organised as follows. Section II analyses our two use cases, GCE and OLPP, to define requirements on dynamic security context management in user-controlled resource provisioning. Section III describes a general model for providing policy-based access control to Grid-based resources or services, and summarises what components of the typical access control infrastructure can be used to mediate a dynamic security context. . Section IV introduces new functionalities and associated components that need to be added to the GAAA Authorization framework and the GAAA toolkit [6, 7] to address the complex network resources provisioning requirements.

Section V provides brief analysis what functionality is available in XACML and SAML to express and handle policy and service/process related security context. Section VI discusses how the Virtual Organisation (VO) concept can be used to create dynamic security associations of users and resources.

The proposed approach and solutions are being developed to respond to both common and specific requirements in the GigaPort-RoN and Collaboratory.nl (CNL)[5] projects and are based on current experience in the EGEE, LCG2 [6], and NextGRID[7] projects.

II. Workflow Control and Dynamic Security Context Management

Providing collaborative environment and access to complex resource such as supercomputer centres and unique experimental equipment is one of major areas of using Grid in industry and in research. To have it interesting to business applications it should adopt customer driven business/provisioning model.

Typical GCE use cases require that the collaborative environment:

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

Currently these problems are addressed in a manual way by hand-configuring and managing user accounts and instruments. This is resulted in slow adaptation of the working space, a high administrative overhead and overly complex management. 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 [8] 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.

In many cases of the distributed collaborative environment there is a need to provide dedicated high-speed communication channels for the experiment that may last from few hours to few months. This can be done with the bandwidth on-demand (BoD) provisioning or OLPP in particular which also require dynamic security context management.

Typically provisioning process comprises of 4 steps: resource lookup, complex resource composition (including options), reservation of individual resources and their association with the reservation ID/ticket, and finally provisioning or delivery. The reservation and optionally delivery stages may require execution of complex procedures that may also request individual resources authorization. This can be achieved by using workflow as a framework for combining executive procedures and security services with necessary security context management.

Current GAAA Authorization framework implementation for BoD provisioning uses a driving policy for combined bandwidth request authorization and network equipment control. However, such approach has manageability problems, and one of such problems can be in combining external policy components and/or making calls to external decision making points depending on master driving policy flow/sequence.

One of suggested solutions for this issue is to separate policy evaluation and workflow management and combining them in the workflow decision points. This approach actually uses workflow as the upper layer abstraction of the overall provisioning process and can be used for creating dynamic Grid services and managing internal service operation.

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 [9, 10].

Currently available BPEL and SWMS implementations can simplify a major part of the provisioning process automation;

[5] http://www.collaboratory.nl/
[6] http://lcg.web.cern.ch/LCG/
[7] http:// www.nextgrid.org/

their integration and extension with the access control and other security services will allow for providing reliable dynamic services.

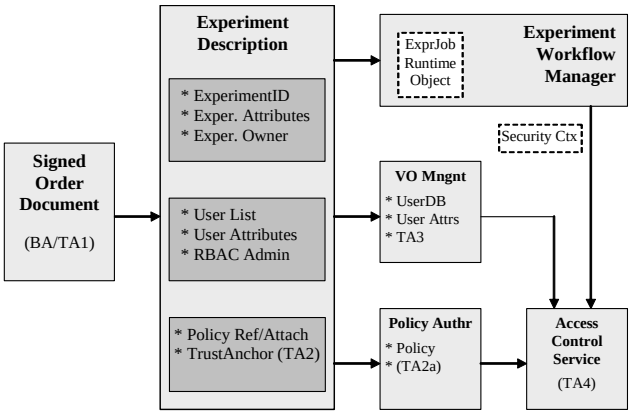

Figure 1. Workflow and security context in GCE

Figure 1 shows an example how the Experiment description can be used in the overall experiment management and for providing necessary configuration and context information for all experiment related services in a typical GCE application [4]. The Experiment description is created by the experiment owner as a semantic object on the basis of signed agreement and can be used as the scope for developing a workflow with standard workflow design tools. 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.

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 trust relations 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 solution for managing dynamically established trust relations between member organisations that are in the process of performing a specific experiment.

III. Access Control in Grid-based applications

Fine-grained access control in typically interactive services in a GCE can be achieved using the Role-Based Access Control (RBAC) authorization model, which generally consists of major functional components that include: Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Authority Point (PAP) [11]. 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 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 Authorization (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 be 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 authorization model and (should be known) service access control policies.

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 document 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 AuthN service and Attribute Authority that can be also a function of the Identity Provider (IdP).

In order to optimize performance of the distributed access control infrastructure, the Authorization service may also issue authorization tickets (AuthzTicket) that confirm access rights. They are based on a positive decision from the Authorization system and can be used to grant access to subsequent similar requests that match an AuthzTicket. AuthzTicket can be used for AuthZ session management and in this way providing a session context to the service request evaluation. To be consistent, AuthzTicket must preserve the full context of the authorization 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 [12] 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). Additional integration of the access control with the workflow management discussed in this paper will allow dynamic security context management and may simplify management of multiple policies.

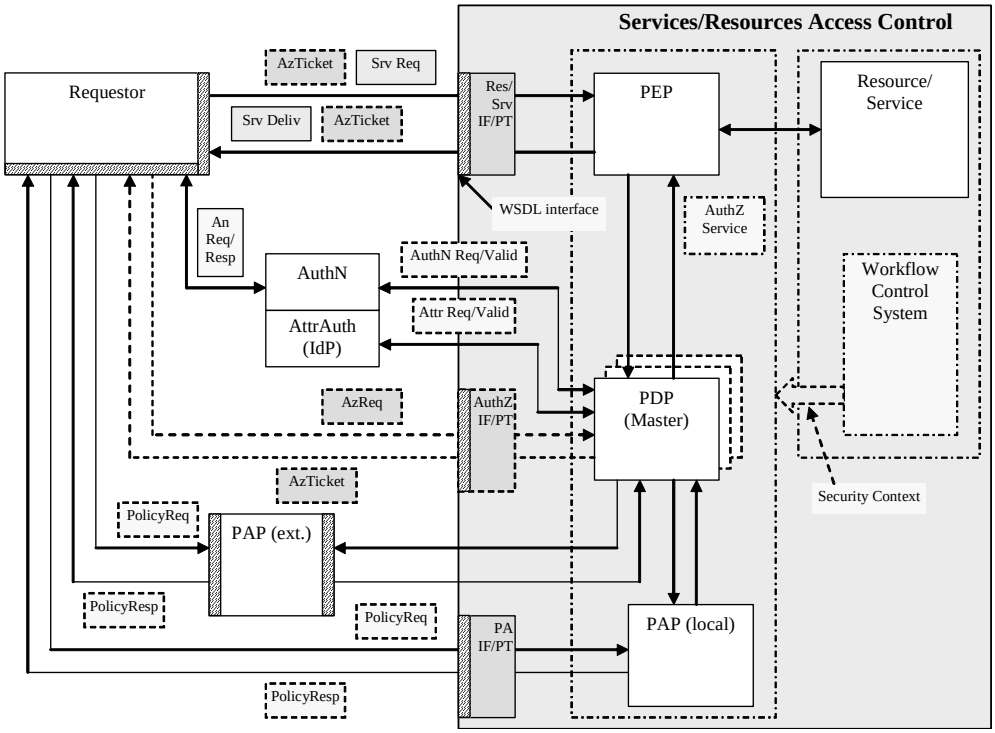

Figure 2. Main interacting components involved in access control in a typical Grid-based collaborative application

The following components of the general access control infrastructure can be used to mediate a dynamic security context:

- Service and requestor/user ID/DN format that should allow for both using namespaces and context aware names semantics.
- Attribute format (either X.509/X.521 or URN/SAML2.0 presentation).
- Context aware XACML policy definition using the Environment element of the policy Target element (see section 5 for detailed discussion).
- Security tickets and tokens used for AuthZ session management and for provisioned resource/service identification. In both cases security tickets should contain the full security context and be supported by related AuthZ and provisioning infrastructure.
- Dynamic VO (or other federation) membership credentials (practically can be supported by existing VO management tools – see section 6 for details) or other user and services federations.

IV. Extending GAAA-Authz for Dynamic Security Context Management

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 [7]. GAAA_tk provides basic functionality for the Generic Authentication, Authorization and Accounting (GAAA) Authorization framework described in [6]. 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 allows for complex multi-domain policy evaluation and execution of complex provisioning algorithms.

A. GAAA-AuthZ 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 Triage functionality together with supporting it Cache that provide 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;

- A Policy Information Point (PIP) together with an Attribute Resolver that process request information to prepare it for the evaluation by the PDP handling; they may call-out to related authoritative Policy Authority Points (PAP) and Attribute Authority Service (AAS), which can be a part of the Identity Provider service (IdP);
- A namespace resolver to define/resolve what policy and what attributes should be used for the request evaluation.

- 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);
- 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.

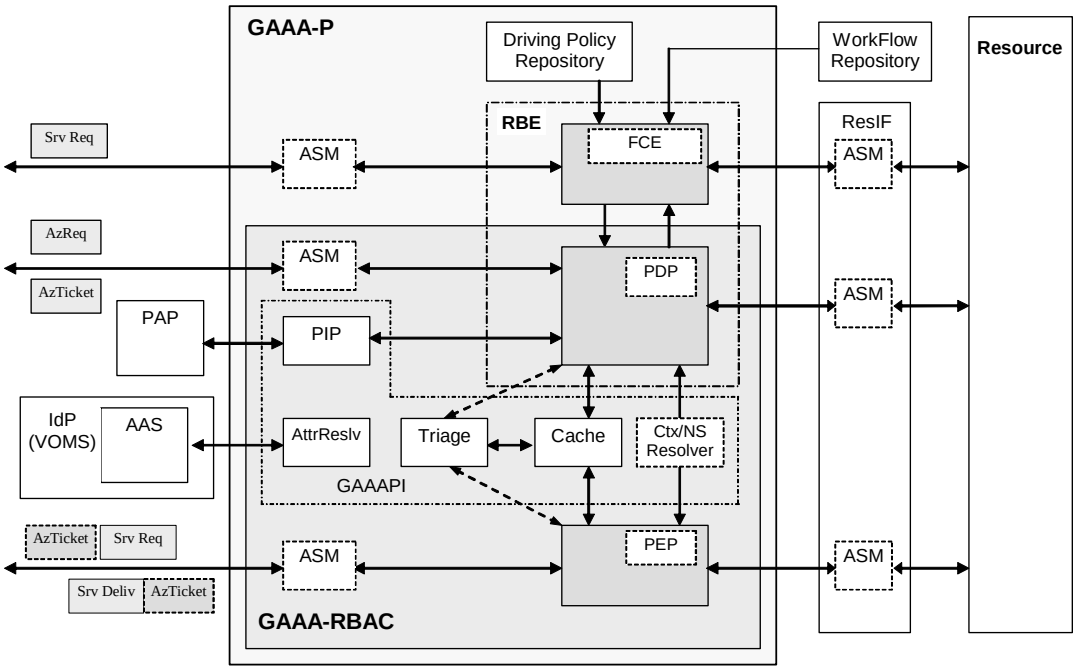

Figure 3. GAAA-RBAC and GAAA-P profiles and main functional components

As a result of its practical implementation (see [9] for typical GCE use case), the GAAA-RBAC functionality was extended with two additional features that are often missing in available access control implementations: authorization 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). In this case, 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;
- resource/service policy evaluation by the PDP that performs request evaluation against the applicable access control policy;
- 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 drives the evaluation and provisioning process. This should also simplify multiple policy combination and avoid possible individual policies conflicts and attribute mismatch.

B. *Integration with the GT4 and gLite Authorization Frameworks*

GT4 Authorization Frameworks (GT4-AuthZ) [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 Authorization PortType [14] that uses SAML as a messaging format. A simple XACML-based PDP is also provided.

gLite Java Authorisation Framework (gJAF) is a component of the gLite security middleware [15]. It inherits compatibility with the early versions of the GT4-AuthZ that should ensure their future interoperability and common use of possible application specific modules. Both the GT4-AuthZ and gJAF services can be called from the SOAP based Grid services by configuring the interceptor module which operates in this case as a virtual PEP module together with the chain.

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 Authorization Framework can be performed in three ways:

(1) using GT4 WS/messaging firmware to provide WS-based access to the GAAA_tk authorization service, thereby allowing easy GAAA_tk integration into different Grid based 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 Authorization Framework functionality such as authorization session management, handling of authorization tickets and tokens, complex XACML policy evaluation, flexible trust domains and request semantics configuration and management.

V. Security context expression in XACML and SAML

eXtensible Access Control Markup Language (XACML) and Security Assertions Mark-up Language (SAML) as two complementary XML-based formats provide a rich functionality for the context information expression. 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]. SAML is a format used for expressing security assertions and related exchange protocols for Authentication, Authorization, and Attribute requests [17].

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.

XACML policy format provides few mechanisms of adding and handling context during the policy selection and request evaluation. First of all, this is the policy selection/resolution that is done based on the Target comprising of the Resource, Action, Subject, and optionally Environment elements. Next, attributes identification and semantics can be namespace aware and used for attributes resolution during the request processing.

Additionally, the special XACML RBAC profile [18] provides extended functionality for managing user/subject roles and permissions by defining separate Permission `<PolicySet>`, Role `<PolicySet>`, Role Assignment `<Policy>`, and HasPrivilegeOfRole `<Policy>`. It also allows for using multiple Subject elements to add hierarchical group roles related context in handling RBAC requests and sessions, e.g., when some actions require superior subject/role approval to perform a specific action. In such a way, RBAC profile can significantly simplify rights delegation inside the group of collaborating entities/subjects which normally requires complex credentials management.

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. The current GAAAPI implementation supports both SAML-based and proprietary XML-based AuthzTicket formats [4, 9].

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 IV).

VI. USING VO FOR DYNAMIC SECURITY ASSOCIATIONS MANAGEMENT

In Grid applications and projects, the concept of a VO is used as a framework for establishing project-related resource sharing and user attributes management [1, 19]. Access to these shared distributed resources is provided based on the VO membership and other VO-related attributes like groups and roles.

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 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 popular VO membership management tool used as a de-facto-standard in current Grid applications is the VO Membership Service (VOMS) [20]. VOMS provides VO-defined attributes for authorization and also 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.

When used in dynamic/on-demand resource/service provisioning, the VO can be used for dynamic user and resource security associations' management. Such VO-based security associations can be created based on the provisioning/service agreement and naturally integrated with the workflow management system.

VII. CONCLUSION AND FURTHER DEVELOPMENT

The results presented in this paper are the part of the ongoing research and development of the generic AAA Authorization 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 cooperation with other project/research partners 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.

The use cases discussed in the paper allowed us to identify the major required functionality to support dynamic security context. Adding workflow management as a component of an integrated security infrastructure allows separation of security functionality related to traditional security middleware from those related to business logic, whilst at the same time providing their tight integration.

The workflow management system can provide a changing security context to authorization/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-AuthZ profiles: GAAA-RBAC for collaborative applications and GAAA-P for provisioning. They consist of the majority of the same modules but can operate in different way when handling single requests for service access or complex service provisioning that may require multiple policies and attributes evaluation. GAAA-P is extended with the flow management functionality to handle complex authorization requests (for service provisioning) that require conditional and multi-step evaluation.

The AuthZ ticket and token handling functionality allows for performance optimisation and supports authorization session management. Further development includes extended AuthZ ticket format (both proprietary and SAML-based) to support multidomain provisioning scenarios and hierarchical resource and policy administration. Additional features include delegation and extended session context.

Suggestions are given how XACML and SAML can be used for expressing and handling security context. Additionally, paper provides suggestions about using the VO concept and available VO management tools and infrastructure for dynamic user and resource security associations. In this case the VO is used for defining VO-related policies and attributes.

Targeting both Grid and non-Grid communities the paper provides suggestions about integration of the GAAA toolkit and GT4 Authorization framework to benefit both solutions and application areas by using rich GT4-AuthZ functionality in evaluating Grid specific credentials and add specific GAAA-AuthZ functions for complex resource provisioning and collaborative applications, such as complex XACML-based policies evaluation, performance optimisation and authorization session management with AuthZ tickets and tokens, and flexible multidomain security and namespace configuration.

The authors believe that the briefly described here research and development in the area of providing flexible dynamic access control architecture will be useful for wider research and development community working in the area of the security-enabled resource provisioning in dynamic distributed environment that need to combine business process management and security services.

REFERENCES

[1] Foster, I. et al, "The Open Grid Services Architecture, Version 1.0", Global Grid Forum, GFD-I.029, January 2005, available from http://www.ggf.org/documents/GFD.30.pdf

[2] Foster, I. et al, "Open Grid Services Architecture Use Cases" , Global Grid Forum, GFD-I.029, October 2004, available from http://www.ggf.org/documents/ GFD.29.pdf

[3] Gommans, L. et al, "Applications Drive Secure Lightpath Creation across Heterogeneous Domains", Special Issue "*IEEE Communications Magazine, Feature topic Optical Control Planes for Grid Networks: Opportunities, Challenges and the Vision*", March 2006.

[4] Demchenko, Y., L. Gommans, C. de Laat, B. Oudenaarde, A. Tokmakoff, R. van Buuren, "Policy Based Access Control in Dynamic Grid-based Collaborative Environment," in *Proc. The 2006 International Symposium on Collaborative Technologies and Systems*, Las Vegas, NV, USA, May 14-18, 2006. IEEE Computer Society, ISBN: 0-9785699-0-3, pp. 64-73.

[5] Y. Demchenko, L. Gommans, B. van Oudenaarde, "Filling the Gap with GAAA-P: Gap Analysis of Authorization technologies and solutions for Optical Light Path Provisioning", Gigaport-NG RoN Technical report. [Online]. Available: http://staff.science.uva.nl/ ~demch/analytic/airg-gp6-ron-gap-aaa-12.pdf

[6] 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.

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

[8] Zhiming Zhao et al, "Scientific workflow management: between generality and applicability," in *Proc. The 5th international conference on quality software*, Melbourne, Australia, Sep. 19 -20, 2005.

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

[10] *Business Process Execution Language for Web Services version 1.1*, Updated February 1, 2005. [Online]. Available: http://www-128.ibm.com/developerworks/library/ specification/ws-bpel/

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

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

[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. [Online]. Available: https://forge.gridforum.org/projects/ogsa-authz

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

[16] *eXtensible Access Control Markup Language (XACML) Version 2.0*, OASIS Standard, 1 February 2005. [Online]. Available: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[17] *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS Standard, 15 March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

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

[19] Demchenko, Y., et al., "VO-based Dynamic Security Associations in Collaborative Grid Environment," in *Proc. The 2006 International Symposium on Collaborative Technologies and Systems*, Las Vegas, NV, USA, May 14-18, 2006. IEEE Computer Society, ISBN: 0-9785699-0-3, pp. 38-47.

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