Dynamic Security Context Management in Grid-based Applications

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

[#]System and Network Engineering Group, University of Amsterdam
Kruislaan 403, 1098SJ, Amsterdam, The Netherlands
[1]demch@science.uva.nl, [2]mulmo@pdc.kth.se, [3]lgommans@science.uva.nl,
[4]delaat@science.uva.nl, [5]wan@science.uva.nl
[*]Center for Parallel Computers, Kungliga Tekniska högskola
SE-100 44 Stockholm, Sweden

Abstract

This paper summarises ongoing research and recent results on the development of flexible access control infrastructure for complex resource provisioning in Grid-based collaborative applications and on-demand network services provisioning. The paper analyses the general access control model for Grid based applications and discusses what mechanisms can be used for expressing and handling dynamic domain or process/workflow related security context. Suggestions are given what specific functionality should be added to the Grid-oriented authorization frameworks to handle such dynamic security context. As an example, the paper explains how such functionality can be achieved in the GAAA Authorization framework (GAAA-AuthZ) and GAAA toolkit. Additionally, the paper describes AuthZ ticket format for extended AuthZ session management. The paper is based on experiences gained from major Grid based and Grid oriented projects such as EGEE, Phosphorus, NextGRID, and GigaPort Research on Network.

Keywords: Dynamic Grid services; Grid middleware; Complex Resource Provisioning, Policy Based Access control; Authorisation; Dynamic security context; Authorisation session; Generic AAA Authorisation Framework; Globus Toolkit Authorisation Framework

1. 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.

Grid infrastructure and applications rely on the Grid middleware that 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. Recently, Grid middleware being developed in the framework of large international projects such as EGEE[1], OSG[2] and Globus Alliance[3] 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].

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 without requiring higher service administration and management overhead. 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.

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

The paper summarises recent works and publications by authors that are focused on building dynamic access control infrastructure for the general Complex Resource Provisioning (CRP) of which the two are taken as the most important use cases: Optical Light Path Provisioning (OLPP) [3] and Grid-based Collaborative Environments (GCE) [4].

The proposed solutions are also targeted to be easy integrated with the application specific and upper layer workflow or resource management systems that allows adding business logic to the provisioning process and automate the user-provider relationship management, e.g. through the negotiation and establishment of a Service Level Agreement (SLA) at the reservation stage and enforcing SLA at the run-time.

The paper is organised as follows. Section 2 analyses the two mentioned above use cases, GCE and OLPP, to define requirements on dynamic security context management in user-controlled resource provisioning. Section 3 describes a general model for providing policy-based access control to Grid-based resources, and summarises what components of the general access control infrastructure can be used to mediate a dynamic security context. Section 4 introduces new functionalities and associated components that need to be added to the GAAA Authorization framework and the GAAA toolkit [5, 6] to address the CRP requirements to dynamic security services. Section 5 describes briefly the AuthZ ticket datamodel and format that allows for the extended AuthZ session security context management during the resource provisioning and access stages.

The proposed approach and solutions are being developed to respond to both common and specific requirements in the SURFnet GigaPort Research on Network (GigaPort-RoN)[4] and Phosphorus[5] projects and are based on current experience in the EGEE and NextGRID[6] projects.

2. Complex Resource Provisioning and Dynamic Security Services

One of the major motivators for adoption of Grid computing in industry and research has been the provisioning of cross-organisational collaborative environments and access to complex distributed resources, such as supercomputer centres and unique experimental equipment. Moving to more business oriented applications and on-demand resource provisioning will require adoption of a customer-driven business/provisioning model which in its own turn will rely on dynamic Grid and Web services.

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 security 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 results in slow adaptation to changes in personnel and/or resource availability, and incur a high administrative overhead and overly complex management. For many experiments there is a need to execute and/or manage a complex workflow that may have effects on the scope or context of some security services (including access control policies) at different stages in the experiment. For instance, when providing access control during a long-running or multi-stage experiment, the security context (e.g., the data access policies, team members and/or roles) may change over time. This means that access control service should be capable to receive and interpret workflow defined dynamic security context. The paper [7] proposed the domain-based resource management and access control models for a typical distributed Virtual Laboratory (VL) organisation and operation that includes factory facilities, VL assigned instruments and resources together with binding them project and/or experiment agreement. For the purpose of consistent security context management, the paper introduced two other dynamically created security associations (acting as lower level security domain): experiment session and collaborative session, that simplifies the dynamic security context management when accessing the VL based collaborative applications.

For many distributed collaborative applications, 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 requires dynamic security context management.

The typical on-demand resource provisioning includes 2 major stages: resource reservation and the reserved resource access or consumption. In its own turn, the reservation and allocation stage includes 4

[4] http://ron.gigaport.nl/
[5] http://www.ist-phosphorus.eu/
[6] http:// www.nextgrid.org/

basic steps: resource lookup, complex resource composition (including alternatives), reservation of individual resources and their association with the reservation ticket/ ID, and finally delivery or deployment/allocation. The reservation and delivery stages may require execution of complex procedures that may recursively request other resources, whose authorization policy depends on other parts of the provisioning (e.g., you can only reserve a lightpath if you also have access to the telescope or video conferencing equipment). This can be achieved by using workflow as a framework for combining executive procedures and security services with the 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 [3]. 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.

The recent paper by authors [8] proposed to separate policy evaluation from the workflow management, and instead combining them at the workflow decision points. This approach allows using workflow as the upper layer abstraction of the overall provisioning process for on-demand provided Grid based resources and services that may span multiple administrative and security domains and have separately managed security policies.

3. Access Control in Grid-based Applications and Dynamic Security Context

Fine-grained access control in typically interactive services in Grid based applications can be achieved using the Policy-Based Access Control (PBAC) authorization model, which generally consists of major functional components that include: Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Authority Point (PAP) [9]. In PBAC, user/requestor access rights are defined by roles in a form of user attributes, and a separately managed access control policy that define what roles are allowed to perform what actions on the resource.

Figure 1 below shows the 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 for the duration of AuthZ session. 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 in a multidomain CRP may require a combination of multiple policies and also multi-level access control enforcement, which may also take place when combining newly-developed and legacy access control systems into one integrated access control solution. In the workflow driven scientific collaborative applications the experiments may apply different policies and require different user credentials depending on the stage of the experiment. In this case the access control system should allow integration with the workflow management system which in its own turn can be used for the dynamic security context management and for multiple policy decisions combinations.

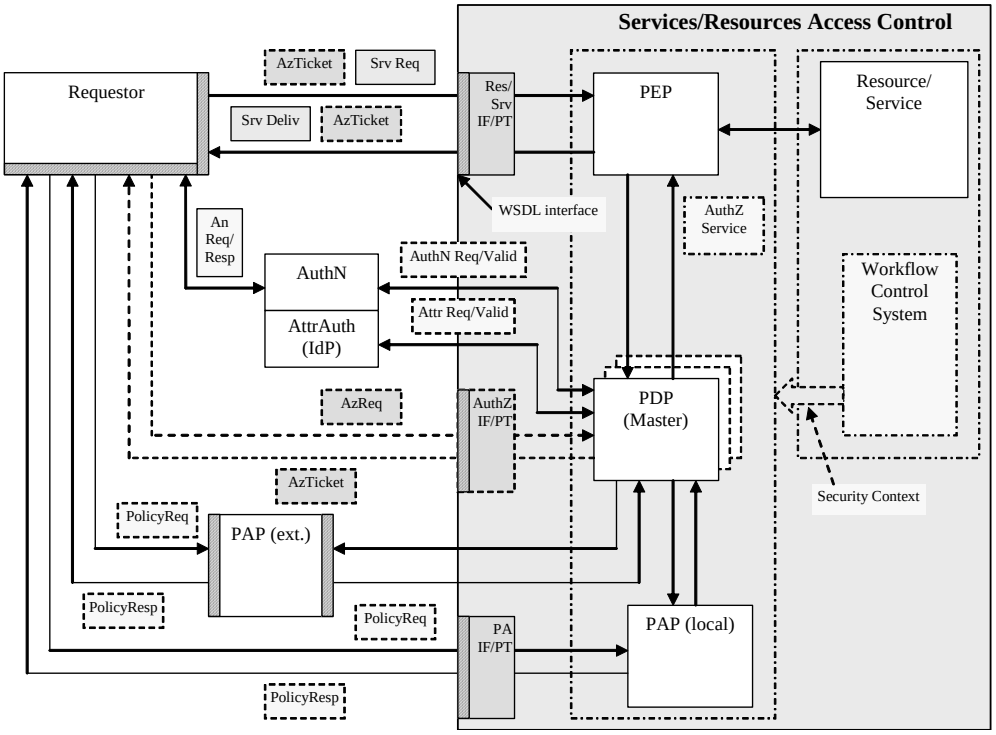

Figure 1. Main interacting components involved in access control in a typical Grid-based application (all component services are available via Web Services PortType (PT) described in WSDL format)

When considered for the access control in CRP applications, 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) that can support domain aware format and semantics.
- 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. This can be supported by existing VO management tools such as VO Membership Service (VOMS) [10], or other more general Identity federation infrastructures like Shibboleth [11].

Dynamic security context should be supported by appropriate access control policy model that allows adding context related information to the typically static policy rules. This kind of functionality is available in the XML-based eXtensible Access Control Markup Language (XACML) [12]. An XACML policy is defined for the so-called target triad “Subject-Resource-Action” (S-R-A) which can also be completed with the Environment element (S-R-A-E) 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. The Obligations information that is returned by the XACML PDP can be used for providing security context for the following policy decisions as the Environment information.

4. Extending GAAA-AuthZ for Dynamic Security context management

The above-described functionality can be provided by the GAAA Toolkit (GAAA_tk) [6] that implements the basic functionality of the generic Authentication, Authorization and Accounting (GAAA) Authorization framework as described in RFC2904 [5]. 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.

4.1 GAAA-AuthZ Implementation with the GAAA Toolkit

Figure 2 shows the GAAA_tk structure that contains the following functional components, which are related to two basic profiles (GAAA-RBAC and GAAA-P). 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.

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 that providse an initial evaluation of the request, including the validity of the provided credentials. A supporting Cache simplifies and speeds up this process. 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) that processes request information to prepare it for the evaluation by the PDP handling; if necessary, it can extract policy from related authoritative Policy Authority Points (PAP). It may also use an Attribute Resolver to obtain additional attribute related information from the external Identity Provider service (IdP) through its Attribute Authority Services (AAS);
- A namespace resolver to define/resolve what policy and what attributes should be used for the request evaluation.

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

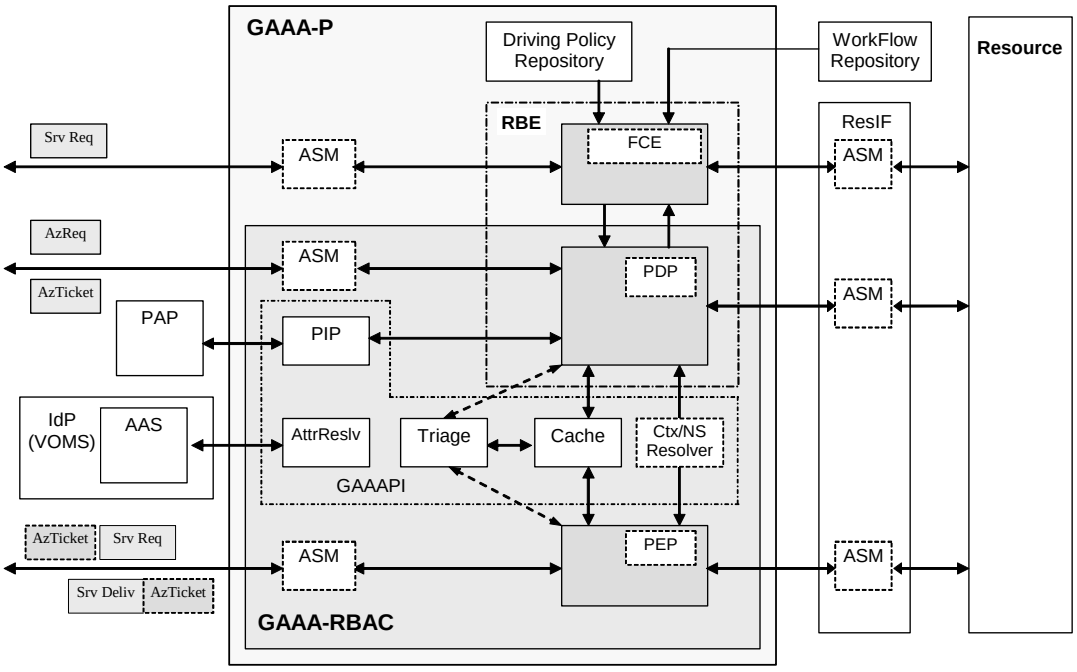

Figure 2. GAAA-RBAC and GAAA-P profiles and main functional components

As a result of its practical implementation (see [4, 7] for typical GCE use case), the GAAA-RBAC functionality was extended with two additional features that are often missing in existing 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 the access control system(s) 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 can also simplify multiple policy combination and avoid possible individual policies conflicts and attribute mismatch.

4.2 Integration with the GT4 and gLite Authorization Frameworks

The Globus Toolkit Web Services Authorization Framework (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 authorization. GT-AuthZ supports external XACML based PDP callouts using SAML-XACML interface and assertions [14] A simple internal 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 an interceptor module that operates as a PEP.

GAAA_tk is being developed to be compatible with both the GT4 and gLite toolkits, but with a goal to provide the necessary functionality for collaborative and CRP 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 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-AuthZ functionality such as authorization session management, handling of authorization tickets and tokens, complex XACML policy evaluation, flexible trust domains configuration and management.

5. AuthZ Ticket Format for Extended AuthZ Session Security Context Management

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 content compared with the Request. 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).

As discussed in the previous section, there are two types of sessions in the proposed CRP model that require security context management: provisioning/reservation session, and access or collaborative session. Although provisioning session may require wider security context support, both of them are based on the (positive) AuthZ decision, may have similar AuthZ context and will require similar functionality when considering distributed multi-domain scenarios.

Current AuthzTicket format and its implementation in the GAAA-AuthZ support extended functionality for distributed multidomain hierarchical resources access control and user roles/permissions management, in particular, administrative policy management (as defined in XACML 3.0 Administrative policy profile [16]), capabilities delegation and conditional AuthZ decision assertion (to support XACML policy obligations). The semantics of AuthzTicket elements is defined in such a way that allows easy mapping to related elements in other XML-based and AuthZ/AuthN related formats, like XACML [12] or the Security Assertion Markup Language (SAML) [17].

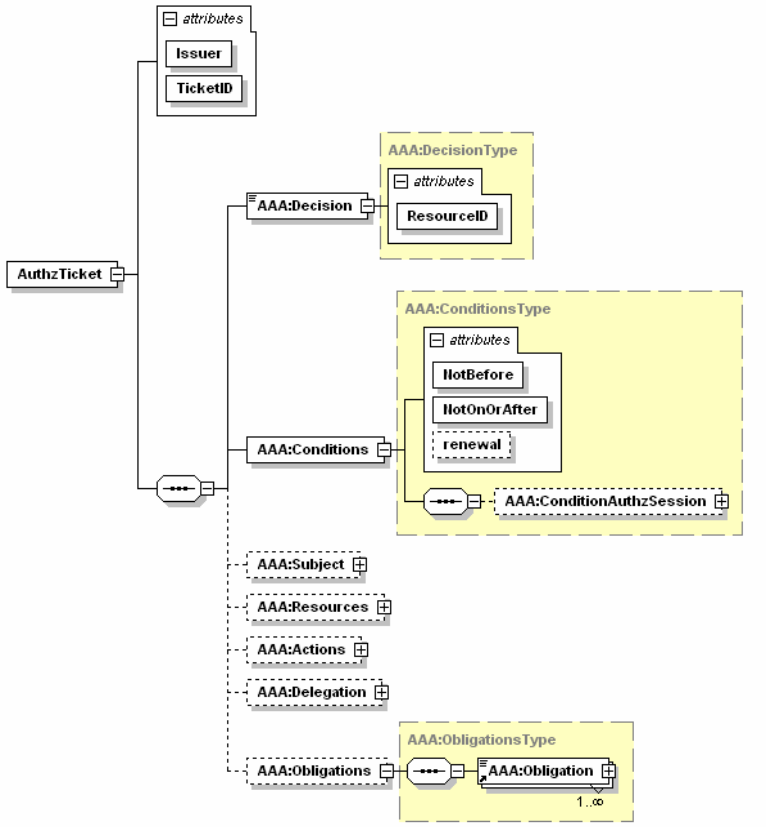

Figure 3. The AuthzTicket data model and top elements.

Figure 3 illustrates the AuthzTicket data model and shows the top elements. The AuthzTicket contains the following major groups of elements that allow for extended AuthZ session security context management:

- The `Decision` element that holds the PDP AuthZ decision bound to the requested resource or service expressed as the `ResourceID` attribute.
- The `Actions/Action` complex element contains actions which are permitted for the Subject or its delegates.
- The `Subject` complex element contains all information related to the authenticated Subject who obtained permission to do the actions, including sub-elements: `Role` (holding subject's capabilities), `SubjectConfirmationData` (typically holding AuthN context), and extendable sub-element `SubjectContext` that may provide additional security or session related information, e.g. Subject's VO, project, or federation.
- The `Delegation` element allows to delegate the capabilities defined by the AuthzTicket to another Subjects or community. The attributes define restriction on type and depth of delegation

- The `Conditions` element specifies the validity constrains for the ticket, including validity time and AuthZ session identification and additionally context. The extensible `ConditionAuthzSession` element provides rich possibilities for AuthZ context expression.
- The `Obligations/Obligation` element can hold obligations that PEP/Resource should perform in conjunction with the current PDP decision.

The semantics of AuthzTicket elements is defined in such a way that allows easy mapping to related elements in SAML and XACML. First three elements the `Decision`, the `Actions/Action`, and the `Subject` have direct mapping to related SAML elements. Other AuthzTicket elements the `Delegation`, the `Conditions`, and the `Obligations/Obligation` element, which is originated from XACML, can be implemented as extensible element of the SAML `Condition` element.

The current GAAAPI implementation supports both SAML-based and proprietary XML-based AuthzTicket formats. The AuthzTicket is digitally signed and cached by the Resource's AuthZ service. To reduce communication overhead when using AuthzTicket for consecutive requests validation, the associated AuthzToken can be generated of the AuthzTicket. The AuthzToken may contain just two elements: `TokenID = TicketID` and `TokenValue = SignatureValue`, needed for identification of the cached AuthzTicket.

6. 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, Phosphorus, 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 in policy-based access control in Grid-based applications. The paper identified what mechanisms can be used for expressing and communicating dynamic security context in policy-based access control systems. It was shown that most of these mechanisms can be supported by using two complimentary XML-based standards XACML and SAML.

The paper proposed to use the AuthZ ticket as a semantic construct to express and communicate AuthZ context in multidomain process execution and resource provisioning, in particular, for securing resource reservation and ensuring secure access to the reserved resources. The AuthZ ticket and token handling functionality allows for performance optimisation and supports authorization session management. The paper describes the current design of the XML based and SAML compatible AuthZ ticket format that provides rich functionality for AuthZ session and security context management in complex multidomain resource provisioning, in particular for network resource provisioning. Further development is suggested to extend AuthZ ticket functionality and format (both proprietary and SAML-based) to support different provisioning scenarios and different resource models [18].

The proposed implementation is based on the special GAAA-AuthZ profiles: GAAA-RBAC profile for collaborative applications, and GAAA-P profile for provisioning. They consist of the majority of the same modules but 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 may require conditional and multi-step evaluation.

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 trust configuration and management.

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.030, 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] 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.

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

[7] Demchenko, Y., Leon Gommans, Cees de Laat, Rene van Buuren, "Domain Based Access Control Model for Distributed Collaborative Applications", in Proc. *The 2nd IEEE International Conference on e-Science and Grid Computing*, December 4-6, 2006, Amsterdam.

[8] Demchenko, Y., L. Gommans, C. de Laat, A. Taal, A. Wan, O. Mulmo, "Using Workflow for Dynamic Security Context Management in Complex Resource Provisioning", 7th IEEE/ACM International Conference on Grid Computing (Grid2006), Barcelona, September 28-30, 2006, pp.72-79.

[9] ITU-T Rec. X.812 (1995) | ISO/IEC 10181-3:1996, Information technology - Open systems interconnection - Security frameworks in open systems: Access control framework. [Online]. Available: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.812-199511-I!!PDF-E&type=items

[10] Virtual Organization Membership Service (VOMS). [Online]. Available: http://infnforge.cnaf.infn.it/voms/

[11] Shibboleth Attribute Authority Service. {Online}. Available: http://shibboleth.internet2.edu/

[12] *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

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

[14] *SAML 2.0 Profile of XACML 2.0, Version 2*. OASIS Working Draft 2, 26 June 2006. [Online]. Available: http://docs.oasis-open.org/xacml/2.0/xacml-2.0-profile-saml2.0-v2.zip

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

[16] *XACML 3.0 administrative policy*, OASIS Draft, 10 December 2005. [Online]. Available: http://docs.oasis-open.org/access_control

[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] Demchenko, Y., L. Gommans, C. de Laat, "Using SAML and XACML for Complex Authorisation Scenarios in Dynamic Resource Provisioning”, The Second International Conference on Availability, Reliability and Security (ARES 2007), April 10-13, 2007, Vienna.