Using SAML and XACML for Complex Resource Provisioning in Grid based Applications

Yuri Demchenko, Leon Gommans, Cees de Laat
System and Network Engineering Group, University of Amsterdam
{demch, lgommans, delaat}@science.uva.nl

Abstract

This paper presents ongoing research and current results on the development of flexible access control infrastructure for complex resource provisioning (CRP) in Grid-based applications. The paper proposes a general CRP model and specifies major requirements to the Authorisation (AuthZ) service infrastructure to support multidomain CRP, focusing on two main issues – policy expression for complex resource models and AuthZ session support. The paper provides suggestions about using XACML and its profiles to describe access control policies to complex resources and briefly describes proposed XML based AuthZ ticket format to support extended AuthZ session context. Additionally, the paper discusses what specific functionality can be added to the gLite Java Authorisation Framework (gJAF), to handle dynamic security context including AuthZ session support. The paper is based on experiences gained from major Grid based and Grid oriented projects such as EGEE, Phosphorus and GigaPort Research on Network.

1. Introduction

Modern e-Science applications are based on Grid-enabled sharing of experimental equipment, computing resources and often require dedicated high speed network infrastructure to enable effective collaboration and distributed computation.

Grid and Web Services [1] allow for resources and user groups virtualisation in a form of the Virtual Laboratories (VL) or Virtual Organisations (VO). Such a virtualisation of resources and users can be created on-demand dynamically, based on experiment or service agreement, and terminated once the experiment has been completed or service/resource delivered or consumed.

When considering a general Complex Resource Provisioning (CRP) model, we investigated different use cases such as Distributed Grid Computing [2], Virtual Laboratories organisation in collaborative e-Science applications [3], and on-demand Optical LightPath Provisioning (OLPP) [4]. Important component of the general CRP infrastructure is AuthZ service infrastructure.

The paper explores the possibilities and presents our experiences with such technologies as XACML and SAML that provide rich functionality for the CRP policy expression and dynamic security context management. The presented research and proposed solutions are specifically oriented for using with the popular Grid middleware being developed in the framework of large international projects such as EGEE[1] and Globus Alliance[2].

The paper is organized as follows. Section 2 describes general CRP model that separates resource reservation, resource allocation, and resource access or consumption stages. The section summarises common requirements to the AuthZ service infrastructure to support different provisioning and AuthZ scenarios in distributed dynamic environment

Section 3 discuses what functionality is available in the XACML specification suite for expressing access control policies for complex distributed resources with different logical organisations (multiple, multiple constrained, and hierarchical). Section 4 describes how the resource domain related dynamic security context and AuthZ session management can be added to the gLite Java AuthZ Framework (gJAF) [5] which is the component of the EGEE gLite middleware. Section 5 describes briefly the AuthZ ticket format that allows for the extended AuthZ session security context management during the resource provisioning and access stages.

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

2. General CRP model and requirements to Authorisation Service

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 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 allocation. The reservation stage may require execution of complex procedures that may also request individual resources authorisation that may belong to different administrative and security domains. This process in general can be controlled by the meta-scheduling system and described as combination of the provisioning workflow and related AuthZ policies for different domains or individual resources.

Figure 1 illustrates major interacting components in the multi-domain CRP that can be applied for both hierarchical domain based resources organisation in VL/VO [3] and multidomain OLPP [4]:

- User/Requestor;
- Target end service or application;
- Multiple Workspace Elements (WSE) (as a component of the VL/VO) or Network Elements (NE) (as component of the OLPP);
- Dynamic Resource Allocation and Management (DRAM) service;
- AAA/AuthZ service controlling access to the domain- related resources.

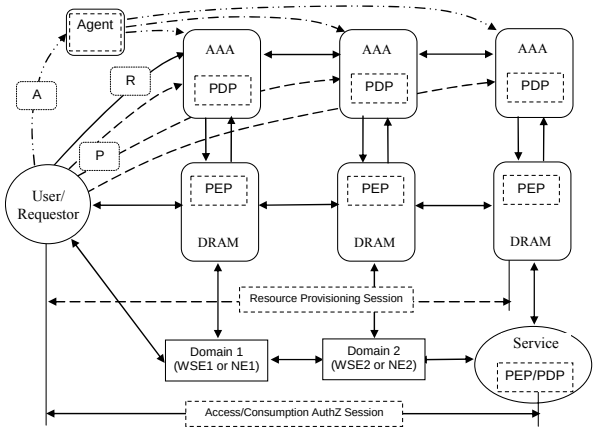

Figure 1. Components involved into CRP and basic sequences: agent (A), relay (R), and polling (P).

Access to the Resource or Service is controlled by the DRAM and protected by the AAA service that enforces Resource access control policy by placing Policy Enforcement Point (PEP) at the entrance of DRAM. Depending on the basic AAA-AuthZ sequence (push, pull or agent) [6, 7], the Requestor can send a Resource access request to the Resource (which is represented by DRAM) or an AuthZ decision request to the designated AAA server which in this case will act as a Policy Decision Point (PDP).

At the access stage, in order to get access to the reserved resources the Requestor will need to present the reservation credentials that can be in the form of AuthZ ticket or token (AuthzTicket or AuthzToken) which will be evaluated by the PEP to grant access to the reserved network element or resource. During the reservation stage the AuthZ ticket can be used for communicating interdomain AuthZ context which is essential for effective decision making.

In the discussed CRP model, domains (as associations of entities) are defined by common policy under single administration, common namespace and semantics, shared trust relations and authorities, etc. Depending on the CRP use case, domains can be hierarchical (like in VL/VO), ordered or tree-based single antecedent (like in OLPP), flat, or organized in the mesh, however all these cases require the same basic functionality from the AuthZ infrastructure to manage domain and session related security context.

The CRP for the hierarchical and distributed resources management requires the following functionality from the AuthZ infrastructure:

- multiple policies processing and combination;
- policy support for different logical organisation of resources, including possible constrains on resource combination and interoperation.
- identities and attributes mapping/converting based on interdomain trust management infrastructure;
- hierarchical roles/permissions management, including administrative policies and delegation;
- extended domain related security and AuthZ session context management;

In the following sections we discuss how the required functionality can be supported by mechanisms available in two complementary XML-based formats Security Assertion Markup Language (SAML) [8] and eXtensible Access Control Markup Language (XACML) [9] and what additional functionality should be added to existing AuthZ frameworks.

3. Using XACML for Policy Expression in CRP

Different CRP scenarios require policies for both complex logically organised resources and for user

flexible roles/permissions management. Most of such functionality can be supported by XACML core specification [9] and its special profiles for RBAC [10] and for multiple [11] and hierarchical resources [12]. Hierarchical policy management and dynamic rights delegation, that are considered as important functionality in CRP, can be supported with the XACML v3.0 administrative policy profile [13].

A XACML policy is defined for the so-called target triad "Subject-Resource-Action" (S-R-A) which can also be completed with the Environment (S-R-A-E) component to add additional context to instant policy evaluation. The XACML policy can also specify the Obligations as actions that must be taken on positive or negative PDP decisions. This functionality is important for accounting in consumable resource provisioning or conditional access control when using pool accounts in computer Grids.

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. 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 to bind the XACML policy to the Resource and handle domain related security context: Target elements that can contain any of S-R-A-E attributes, policy identification attribute IDRef and XACML 3.0 Policy Issuer element [13] which together with the XACML RBAC profile [10] allow also for the policy authority and roles delegation in multidomain hierarchical .scenarios.

The XACML hierarchical resource profile [12] specifies how XACML can provide access control for a Resource that is organized as a hierarchy. The profile introduces new Resource attributes identifiers that may refer to the "resource-ancestor", "resource-parent", or "resource-ancestor-or-self".

Such specific usecase as multidomain OLPP require that resource reservation policy in each successive domain will relay on the previous domain positive AuthZ decision and additionally may also require informing next domain. This can be achieved by using AuthZ or reservation ticket from the previous domain in the Environment element in a simple case. When the sequence is important it can be achieved with the ordered rules and policies combination algorithms defined for the Policy Set or Policy [9].

Examples of XACML policies can be found at the AAAuthreach project page [14].

4. Adding security context management to major Authorisation frameworks

To provide described above functionality for the domain based security context handling and extended AuthZ session management, a number of features should be added to existing Grid oriented AuthZ frameworks. Based on current implementation for the generic AAA Toolkit in the form of GAAAPI package [3, 15] we are considering adding similar functionality for the gLite Java Authorisation Framework (gJAF) [5] that potentially can be integrated with the Globus Toolkit AuthZ framework (GT4-AuthZ) [16].

The gJAF is designed to provide an extensible solution to flexibly handle all the access control policies and information. This is achieved by allowing different pluggable modules to be added and configured in a chain of authorisation modules. gJAF is provided in the form of Java package "org.glite.security.authz" as a part of the gLite middleware.

Figure 2 illustrates the gJAF internal structure and how it is connected to the main service. The gJAF service can be called from the SOAP-based Grid services by configuring the service call or message interceptor module which operates, in this case, as a virtual Policy Enforcement Point (PEP). The core framework includes the following major components: Context Handler (CtxHandler); Policy Information Points (PIPs), Policy Decision Points (PDPs), Policy Authority Points (PAPs), attribute collection chain (PIP-chain), authorisation decision combination chains (PDP-chains), and configuration back-ends.

The first PIP module in the PIP chain is called BootstrapPIP and it performs initials extraction of the S-R-A attributes from the service request MessageCtx and creates the SecurityCtx container of the AuthZ decision request message. Depending on the provided credentials and configuration the PIP chain can contain other PIP to extract and validate different attributes and credentials and may also call to external attribute mapping or validation service, e.g. Shibboleth Attribute Authority Service.

The PDP-chain can also make external PDP call-outs providing an opportunity to integrate other types of PDPєs and policy formats, first of all, XACML-based G-PBox [17] which is another component of the gLite middleware. In this case the G-PBox call-out module should support XACML messaging required by the G-PBox and handle XACML Obligations that can be communicated back to the Grid service via SecurityCtx container of the CtxHandler or back to the requestor in a form of AuthzTicket.

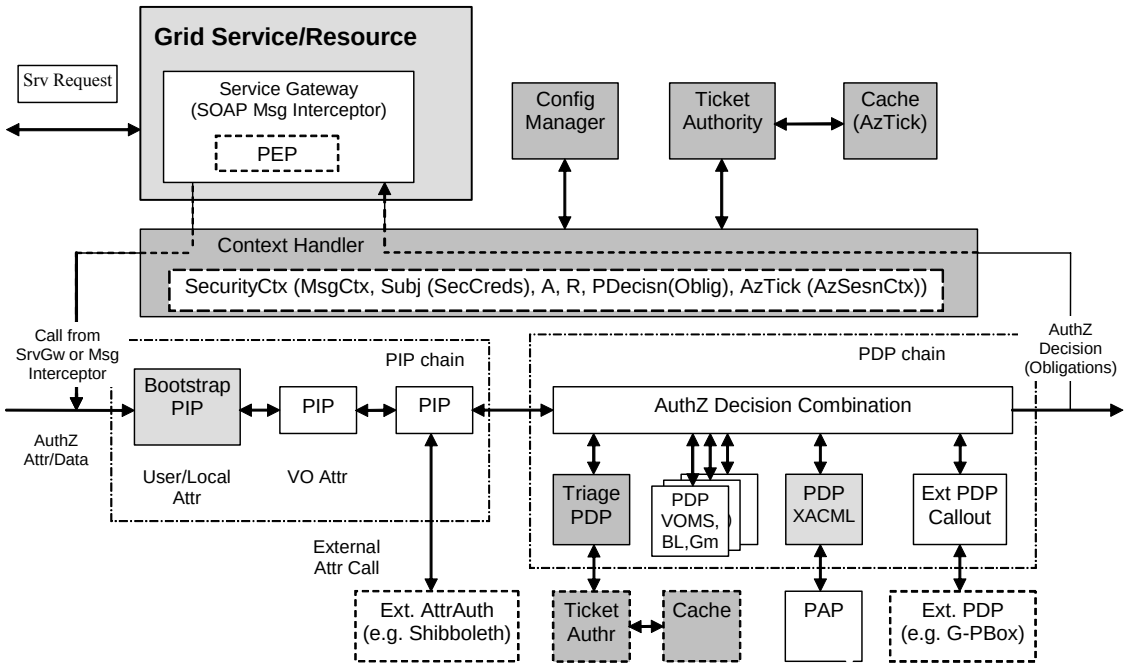

Figure 1. gJAF functional components to support extended security context management in CRP scenarios.

The framework provides general-purpose implementation of different policy decision points such as gridmap-files, black lists and VOMS PDP and is being extended with the XACML PDP. The local configuration of all the policies may be carried out by a custom configuration back-end to easily support legacy configuration formats.

AuthZ session management is supported by the AuthZ ticket and handled by the TriagePDP that provides an initial evaluation of the request against assertions contained in the AuthzTicket and configured as the first PDP in the "permit-override" AuthZ chain. Other AuthZ ticket and session management components include Ticket Authority and Cache that correspondently generate and cache AuthzTicket on the request from the CtxHandler as the result of a positive PDP decision, if this function is configured.

The current implementation in GAAAPI and prospective gJAF implementation support both proprietary XML-based and SAML-based AuthzTicket formats.

5. AuthZ session and AuthZ ticket format

The proposed CRP model suggests two types of AuthZ sessions: provisioning session and access or consumption 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 GAAAPI support extended functionality for distributed multidomain resources access control and user roles/permissions management, in particular, administrative policy management (as defined in XACML 3.0 Administrative policy profile), 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 similar elements in SAML and XACML.

The AuthzTicket contains the Decision related information (including conditions, validity and obligations) and all necessary information to identify reserved Resource, access Subject together with possible delegation conditions, and allowed Actions.

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.

6. Conclusion and Summary

The results presented in this paper are the part of the ongoing research and development of the generic

AAA Authorization framework and its targeted integration with Grid oriented authorisation frameworks such as gJAF and GT4-AuthZ. 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, Phosphorus, and GigaPort Research on Network.

The paper proposed general CRP model that reflects common generic functionality in major CRP use cases in Computer Grids, e-Science collaborations and on-demand network provisioning and specified major requirements to the AuthZ service infrastructure.

In the course of practical implementation, we investigated the use of two popular standards SAML and XACML for complex authorisation scenarios in dynamic resource provisioning across multiple administrative and security domains.

The paper describes proposed XML based AuthzTicket format that is designed to support complex AuthZ scenarios and communicate extended AuthZ session context between (resource or service) domains during the reservation or access stages. Described AuthzTicket format is currently implemented in the GAAAPI package of the AAA Toolkit [14, 15] and being implemented in the gJAF [5]. Additionally, the AuthZ ticket and token handling functionality allows for AuthZ service performance optimization.

The presented research provided a conceptual basis for further extension of the gLite Java Authorisation Framework (gJAF) to support AuthZ session management and allow for extended dynamic security context handling.

The authors believe that the proposed access control architecture for CRP and related technical solutions will also be useful to the wider community has similar problems with managing access control to distributed hierarchically organised resources in dynamic/on-demand services provisioning.

7. References

[1] Foster, I. et al (2006). The Open Grid Services Architecture, Version 1.5. Global Grid Forum. [Online]. Available: http://www.ggf.org/documents/GFD.80.pdf

[2] Hacker, T., B. Athey, A Methodology for Account Management in Grid Computing Environments, Proceedings of the 2nd International Workshop on Grid Computing, November 2001, Denver, Colorado. Lecture Notes in Computer Science, Springer Verlag Press.

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

[4] 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.

[5] gJAF Developer’s guide. [Online]. https://edms.cern.ch/document/501718

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

[7] GFD.38 Conceptual Grid Authorization Framework and Classification. M. Lorch, B. Cowles, R. Baker, L. Gommans, P. Madsen, A. McNab, L. Ramakrishnan, K. Sankar, D. Skow, M. Thompson - http://www.ggf.org/documents/GWD-I-E/GFD-I.038.pdf

[8] "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

[9] "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

[10 "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

[11] "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

[12] "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

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

[14] AAAuthreach Project Information Page [Online]. http://staff.science.uva.nl/~demch/projects/aaauthreach/

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

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

[17] The Grid Policy Box G-PBox. [Online]. Available: http://littleblue.cnaf.infn.it/twiki/bin/view/GPBox/WebHome