Distributed Access Control Management – A XACML-Based Approach

Erik Rissanen[1], David Brossard[2], and Adriaan Slabbert[1]

[1] Axiomatics AB, Electrum 223, 164 40 Kista, Sweden
{erik,adriaan}@axiomatics.com
[2] BT Innovate, Adastral Park, IP5 3RE Martlesham Heath, England
{david.brossard}@bt.com

Abstract. Enterprises are increasingly pervasive with users and services belonging to different domains. Cross-enterprise business collaborations are soaring and so are business relationships with complex access control rules. Business rules no longer come from a single source. There is a need for multiple administrators to define rules that apply to their part of the collaboration. Traditional access control models are not sufficient. This demonstrator illustrates an authorization service developed by Swedish SME Axiomatics. It implements the eXtended Access Control Markup Language (XACML), a policy- and rule-based access control language which allows the expression of fine-grained access control rules in distributed environments.

Keywords: SOA, security, authorization, access control, XACML.

1 Introduction

Distributed access control and authorization services allow access policies to be enforced in a multi-administrative environment. Traditional models tend to rely on a single-administrator model where policies are authored by the same authority within a single domain.

The dynamic nature and level of distribution of the business models typical of service-oriented infrastructures (SOI) [4] mean that one can no longer rely on a set of known users or fixed organizational structures with access to only a set of known systems. Furthermore, access control policies need to be aware of the context within which an access control request is being issued as it can impact the final decision.

The dynamic multi-administrative nature of an SOI necessitates a new model for access control and the development of new models that cater for these characteristics of the infrastructure while combining the best features from role-based, attribute-based, and policy-based access control (RBAC, ABAC and PBAC respectively).

This demonstrator presents the Axiomatics Authorization Service (AuthZ-PDP) and illustrates how it can be used in distributed environments. Axiomatics is also working with OASIS, to drive the evolution of the XACML [2,3] standard.

A demo video can be seen at http://www.gridipedia.eu/gt-axiomatics.html.

L. Baresi, C.-H. Chi, and J. Suzuki (Eds.): ICSOC-ServiceWave 2009, LNCS 5900, pp. 639–640, 2009.

2 System Description

The AuthZ-PDP allows the necessary decision making for distributed enforcement of access policies by multiple administrators, ensuring compliance, accountability and audits. Current access control models are extended with (1) validity conditions for each policy, (2) policy issuance whereby administrators digitally sign the policies they write, and (3) administrative delegation policies that lets an administrator define who can issue policies about what actions on which resources. Key functions include:

- *Policy-based access control*: applicable policies are stored on the system and are analyzed by the PDP. The PDP makes its decision and returns the decision.
- *Constrained Administrative Delegation:* the delegation mechanism is used to support decentralized administration of access policies. It allows an authority (delegator) to delegate all or part of its authority to another user (delegate). The specific authorization can then be delegated further.
- *Obligation*: an obligation is a directive from the PDP to the Policy Enforcement Point (PEP) on what must be carried out before or after access is granted. If the PEP cannot comply with the directive, the granted access will not be realized.
- *Segregation of policy stores*: by means of PDP instantiation, it is possible to have instances of the PDP service that each act as a single standalone PDP.
- *Flexible*: the PDP is standards-based and can be deployed in a variety of ways.

3 Benefits

The innovations that differentiate the solution from other access management capabilities include the delegation of administrative authority: policy authoring and management is controlled by constraint-delegation policies that put constraints on the access management policies that administrators can author and allow the run-time creation of dynamic chains of delegation of administrative authority without assuming prior knowledge of an organization's structure. Authenticity, integrity and accountability are guaranteed: policy authoring rights are granted to issuers whose accountability is enforced by use of digital signatures. This is only possible through the introduction of the Policy Issuer element in XACML and through the rigorous implementation of the standard by the PDP put forward. Lastly, the AuthZ-PDP is context-aware and can be contextualized enabling its use in multi-tenancy scenarios. It can be provisioned in the SaaS pattern.

Acknowledgments. This demonstrator was partly produced within BEinGRID [1].

References

1. The BEinGRID project, `http://www.beingrid.eu`
2. OASIS, XACML 3.0 (core specification and schemas) (May 18, 2008)
3. OASIS, XACML 3.0 administration and delegation profile, (October 10, 2007)
4. Gresty, C., et al.: Meeting customer needs. BT Technology Journal 26(1)