

A Comprehensive Security Architecture for Dynamic, Web Service Based Virtual Organizations for Businesses

Rafael Deitos

Florian Kerschbaum

Philip Robinson

firstname.lastname@sap.com
SAP Research
Karlsruhe, Germany

ABSTRACT

In this paper we propose a security architecture for Virtual Organizations for businesses. The Virtual Organizations we consider are based on web service technology, and are dynamic, i.e. its membership may change frequently throughout its lifetime. The security architecture advances over previous approaches with a new approach for distributed administration based on policy generation which allows local security administrators to remain in complete control over the policies deployed. We show the advantages of our architecture in the case of member replacement.

Categories and Subject Descriptors

D.4.6 [Operating Systems]: Security and Protection—*access controls*; C.2.4 [Computer-Communication Networks]: Distributed Systems—*distributed applications*

General Terms

Design, Security

Keywords

Policy Generation, Security Architecture

1. INTRODUCTION

A VO consists in a collection of individuals and institutions defined according to a set of resource sharing rules [4]. The work in this paper considers VOs with the following properties:

- *dynamic*: VOs evolve during operation, e.g. allowing member replacement.
- *business process driven*: VOs where the interactions are defined by a business process (choreography).
- *web service*: VOs where the shared resources are web services.

A VO management system facilitates the administration and management of such VOs. For details of VO management see [6].

The contribution of the proposed security architecture is that it defines a new model of distributed administration and

control using role-based access control [8] based on policy generation. The policy administration is done by the local security administrators allowing for fine-grained (role-based) policies while the business process (choreography) is been agreed on VO-wide.

2. RELATED WORK

Other approaches for the authorization challenge in VOs have been proposed in the literature. KeyNote [1] and PERMIS [2] do not address the challenge of distributed management of policies, but were rather designed for one trust domain. Akenti [9] focuses on the policy decision as well and leaves the administration question open, but offers the possibility for delegation. CAS [5] and VOMS [3] are designed to be used in distributed administered VOs.

3. SYSTEM ARCHITECTURE

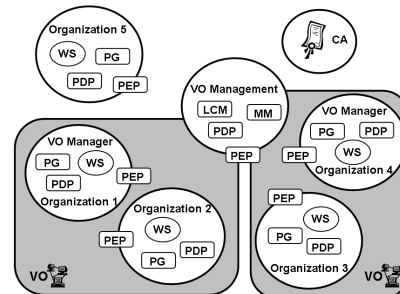


Figure 1: System Architecture

The VO infrastructure is depicted in Figure 1 and consists of the following components:

- **Web Service (WS)**: This is the resource (web service) offered by an organization to the other participants in a VO.
- **Policy Enforcement Point (PEP)**: The PEP intercepts all web service access and forwards the extracted attributes to the PDP before forwarding the message.
- **Policy Decision Point (PDP)**: The PDP makes the access control decision based on the given attributes and a set of policies.

- **Policy Generator (PG)**: The PG retrieves the choreography from the lifecycle manager. A choreography is the description of the flow of cross-organization interactions, i.e. web service calls. It then, with the input of the role the organization, derives the access control policies for the web service. Details of the derivation algorithm can be found in [7].
- **Lifecycle Manager (LCM)**: This service is part of the VO management and it allows the creation and deletion of VOs and also stores the choreography of the VO.
- **Membership Manager (MM)**: The membership manager, as part of the VO Management, assigns organizations to business roles.

4. SECURITY ARCHITECTURE

Each VO has a VO manager that is responsible for all administration tasks. The VO manager can access all administration services (MM and LCM) and perform the necessary operations. VO members may use the query management services (MM) to get information about the VO they are part of, i.e. the list of the members, the status of business partners, the status of the VO.

4.1 Roles

The roles in the policies of the security architecture are the business roles (*BP-ROLE*) as described in the choreography of the VO. To support VO management security, this has to be extended with a second role type for the VO manager (*VOMANAGER*).

In the context of web service security, RBAC policies allow one organization to limit the access to only that role. Compared to capability-based approaches, such as CAS, where the service is exposed to all members of a VO, the organization can now limit the access to a subset of them. Furthermore, the PG can generate these policies automatically from the choreography, minimizing the administration effort.

4.2 Role Assignment and Policy Distribution

The LCM issues an attribute credential attesting the role *VOMANAGER* to the creator of a VO (as a return value of the web service call). Then the VO manager assigns the roles in the business process choreography (*BP-ROLE*) to specific members. For each assignment the VO manager creates an attribute credential with the *BP-ROLE*, the member's identity and the VO identifier and issues it to the member.

Before executing the business process the local security administrators must have installed the access control policies. Each administrator invokes its PG, retrieves the choreography, and verifies the generated policies match his global policies. Note that, the PG generates only the minimal policies necessary for the business process to run, i.e. it conforms to the least privilege principle.

5. MEMBER REPLACEMENT

A common reason to replace a member of a VO is its inability to meet agreed performance requirements, e.g. in our case study if a shipper does not have the resources to ship the goods on time.

The steps required from the security perspective that need to be performed to replace a member are:

1. Remove the organization from its role using the MM and revoke its credentials.
2. Assign a new organization to the role and issue new attribute credentials (using the MM).
3. The new organization receives the attribute credential and invokes its PG.

Note that the steps involve no policy changes except at the new organization (which has been automated).

6. CONCLUSIONS

We present a security architecture for VOs in business. It allows for easy distributed administration using a policy generation approach. The policy generation approach allows for high security using role-based access control, as well as for highly distributed administration where the local security administrator does the administration decision.

7. ACKNOWLEDGEMENTS

The developments presented in this paper were partly funded by the European Commission through the IST programme under Framework 6 grant 001945 to the Trustcom Integrated Project. However, the views expressed in this paper are those of the authors, not those of the consortium.

8. ADDITIONAL AUTHORS

Jochen Haller (SAP Research, Karlsruhe, Germany, email: jochen.haller@sap.com)

9. REFERENCES

- [1] BLAZE, M., FEIGENBAUM, J., AND KEROMYTIS, A. D. Keynote: Trust management for public-key infrastructures. In *1998 Security Protocols International Workshop* (1998).
- [2] CHADWICK, D., AND OTENKO, O. The permis x.509 role based privilege management infrastructure. In *Future Gener. Comput. Syst.* (2003), vol. 19 (2), Elsevier Science Publishers B.V., pp. 277–289.
- [3] DEMCHENKO, Y., COMMANS, L., DE LAAT, C., STEENBAKKERS, M., CIASHINI, V., AND VENTURI, V. Vo-based dynamic security associations in collaborative grid environment. In *Workshop on Collaboration and Security (COLSEC) of The 2006 International Symposium on Collaborative Technologies and Systems (CTS)* (2006).
- [4] FOSTER, I., KESSELMAN, C., AND S.TUECKE. The anatomy of the grid. In *International Journal of High Performance Computing Applications* (2001), vol. 15 (3), pp. 200–222.
- [5] PEARLMAN, L., WELCH, V., FOSTER, I., KESSELMAN, C., AND TUECKE, S. A community authorization service for group collaboration. In *IEEE Workshop on Policies for Distributed Systems and Networks* (2002).
- [6] ROBINSON, P., KARABULUT, Y., AND HALLER, J. Dynamic virtual organization management for service oriented enterprise applications. In *1st International Conference on Collaborative Computing* (2005).
- [7] ROBINSON, P., KERSCHBAUM, F., AND SCHAAD, A. From business process choreography to authorization policies. In *20th Annual IFIP WG 11.3 Working Conference on Data and Applications Security* (2006).
- [8] SANDHU, R., COYNE, E., FEINSTEIN, H., AND YOUMAN, C. Role based access control models. In *IEEE Computer* (1996), vol. 29 (2).
- [9] THOMPSON, M., ESSIARI, A., AND MUDUMBAI, S. Certificate-based authorization policy in a pki environment. In *ACM Transactions on Information and System Security* (2003), vol. 6 (4), pp. 566–588.