

# Access rights and collaborative ontology integration for reuse across security domains <sup>\*</sup>

Martin Knechtel

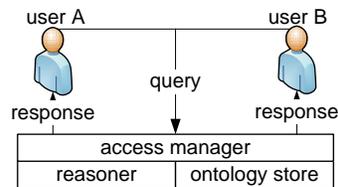
SAP AG, SAP Research CEC Dresden  
Chemnitz Str. 48, 01187 Dresden, Germany  
martin.knechtel@sap.com

## 1 Research Problem

This section gives a description of the overall research problem tackled in context of the Ph.D. and its relevance to the Semantic Web area.

The problem domain for this extended abstract is a collaborative marketplace in the Semantic Web. In the planned pilot 2 of the application scenario *PROCESSUS* of the research program *THESEUS* [1], described products to be sold are Web services. They are traded like goods and described in documents.

Ontologies can be used to define a shared vocabulary with concepts, properties and axioms. By referencing this shared vocabulary in product descriptions, a conceptual navigation over heterogeneous resources is possible.



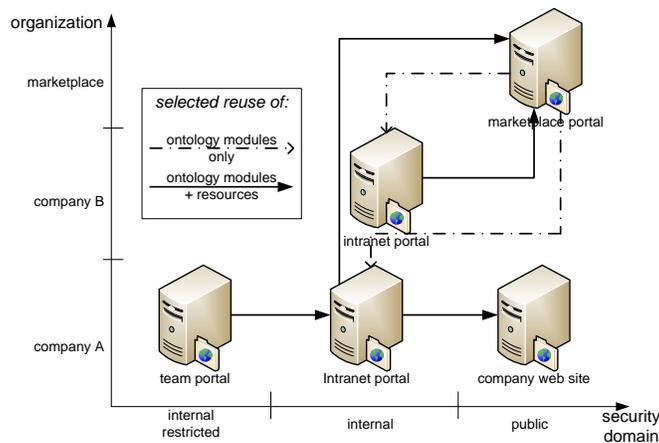
**Fig. 1.** Different responses for the same query, dependent on access rights

This induces that the ontology alone already contains insights about resources' contents. Different user roles are involved when accessing a semantic marketplace, e.g. visitor, customer, high volume customer, provider. Since all of them get different conditions and information detail about products, they get different answers for ontology queries when posing the same question (cf. Fig. 1). Access Control inside ontologies is one focus of the thesis.

A second focus is collaborative ontology integration. Given the functionality to have different views on a ontology for different user roles, one might also

---

<sup>\*</sup> The project was funded by means of the German Federal Ministry of Economy and Technology under the promotional reference "01MQ07012". The author takes the responsibility for the contents.



**Fig. 2.** Reuse of ontology subsets across security domains and different organizations

define a public view on the ontology which can be distributed from a company internal server to a Web marketplace (cf. Fig. 2). In opposite direction, a company can also import the marketplace ontology, which might be based on a product standard like eCl@ss [2].

## 2 Related Work

This section discusses the state of the art in the fields affected by the given scenario.

Semantic content management is studied e.g. for semantic portals [3]. Also wikis can be used for semantic content management [4]. The contributions describe the motivation and implementation of content management with ontology support.

Collaborative Ontology Engineering seems well investigated. Examples are Ontolingua Server [5] and Collaborative Protégé [6]. Since the marketplace is a Web application, it is desirable to edit the ontology directly in the browser [7]. This makes no tool change for contribution and consumption necessary and changes can be tested directly in the application. This thesis' focus is how ontology contextualization can support collaboration.

To reuse parts of an ontology from a company internal context, ontology modularization is involved to decide if a module is complete [8]. In the other direction conservative extensions are extensions of an ontology without changing existing subsumption relations [9]. An interesting question for the thesis is how ontology modularization is influenced by assigned access rights. This is not investigated so far.

Fine grained access control inside ontologies is not well investigated in the research community yet. The contribution [10] presents basic access control meth-

ods and brings them in relation to ontologies. Although this work does not provide technical details, recommendation for authority based access control (ABAC) is given and justified. They propose that hierarchies can be used to inherit rights. According to [11], information about axioms of an ontology can be represented as context. This might be a starting point to represent access rights.

Authorization in other fields like file systems, content management systems, database management systems etc. is modeled by access control lists or by capabilities. Approaches often use hierarchies to inherit access rights. Due to the nature of ontologies, having no tree but a graph structure, access rights inheritance is of limited use. In the subsumption hierarchy a concept can be subconcept of several others, which leads to multiple inheritance. Object relations between concepts may form cycles. And it may be desired that a user can only see the superconcepts but not the subconcepts or the other way round. There is a similiar behaviour commonly used for FTP servers called *chroot jail*.

There are approaches for access rights inside ontologies. While [12] is based on a three-valued semantics and assumes an RDF tree without cyclic references, we want to use Description Logics and not restrict ontology structure to a tree. In [13] the focus is to restrict access on syntactically heterogeneous resources with help of a harmonizing ontology. A security policy is stored separately from the ontology, while we want to integrate it. An own ontology definition is used which is not conform to OWL-DL [14] since e.g. axioms and individuals are missing, while we want to use OWL-DL.

### 3 Contributions

This section describes how the proposed project will advance state of the art and summarizes expected contributions.

From the related work section it seems that context can store information about ontology axioms. The thesis will investigate if this context is suitable to store access rights and collaboration information to support ontology reuse. The following research questions will be subject of the thesis:

1. What is the right granularity for access control within an ontology: axiom, module, whole ontology, others?
2. How are axiom rights propagated to resources?
3. Can ontology axiom rights be derived from resource rights, to improve usability?
4. What effect has access control on reasoning and modularization?

The contribution of the thesis will be a framework to answer the conceptual questions, and an implementation to demonstrate the results. Therefore a conception and a syntactical representation of access rights will be developed. One candidate is to save context within an ontology with annotation properties according to [11]. The OWL1.1 standard will allow annotation properties for axioms and reference by axiom URI. This allows fine grained access control

similar to XML query languages. In the following example the URI is printed in brackets following the axiom.

$$\begin{aligned} & \textit{DesignDocument} \sqsubseteq \textit{Document} \text{ [} \textit{axiom1} \text{]} \\ & \textit{access}(\textit{axiom1}, \textit{companyInternal}) \\ & \textit{access}(\textit{DesignDocument}, \textit{companyInternal}) \end{aligned}$$

Argumentations for axioms and other ontology elements can be recorded analogously. In further processing steps the ontology can be stripped down to a version which only contains elements for public use and is therefore contextualized. But this naive syntactic process will not be enough since the remaining axioms may not make sense alone. The implications of access rights assignment concerning rights inheritance and ontology modularization will be investigated.

## 4 Evaluation

This section describes the methodology used to evaluate and validate results of the project.

In the above mentioned application scenario *PROCESSUS*, different user roles will get access to different parts and granularity level of the ontology. This offers an evaluation opportunity for the thesis' results.

Also collaborative ontology integration might be evaluated in the application scenario, since product descriptions on the marketplace have to be imported from somewhere. They might be interpreted as a subset of the company internal resources and ontology. It is a subset because, whitepapers and other marketing documents are intended to be made publicly available whereas design documents and test protocols which reference the same product are not.

## 5 Work Plan

This section sketches the different stages of the project and differentiates between current status, work in progress and planned future work.

**Results achieved.** The overall thesis work time is planned to be three years.

Six months have passed so far. Currently the idea outline exists as presented in this abstract.

**Current work.** Current work is to investigate the two considered aspects of ontology reuse on behalf of an example case. Next planned step is to finish a paper in 2008-07 to present a first concept and a deeper related work analysis than given in this extended abstract.

**Planned work.** Further coming steps are the following. Until 2008-08 a first draft of the exposé is planned. Up to 2008-10 the structure of the manuscript and potential diploma thesis topics are formulated. Until 2009-10 the conceptual part of the thesis shall be finished, to have time for implementation until 2010-05. The thesis manuscript is planned to be finished in 2010-09.

## References

1. THESEUS research program, "PROCESSUS - optimisation of business processes." available at <http://theseus-programm.de/scenarios/en/processus>, retrieved March 7, 2008.
2. M. Hepp and J. de Bruijn, "GenTax: A generic methodology for deriving OWL and RDF-S ontologies from hierarchical classifications, thesauri, and inconsistent taxonomies," in *ESWC' 07: Proceedings of the 4th European Semantic Web Conference*, pp. 129–144, 2007.
3. J. Hartmann and Y. Sure, "An infrastructure for scalable, reliable semantic portals," *IEEE Intelligent Systems*, vol. 19, pp. 58–65, 5 2004.
4. M. Krötzsch, D. Vrandečić, and M. Völkel, "Semantic MediaWiki," in *ISWC '06: Proceedings of the 5th International Semantic Web Conference*, (Athens, GA, USA), pp. 935–942, Springer, 11 2006.
5. A. Farquhar, R. Fikes, and J. Rice, "The Ontolingua server: a tool for collaborative ontology construction," *International Journal of Human-Computer Studies*, vol. 46, no. 6, 1997.
6. Stanford University, "Protégé 3.3.1 ontology editor." available at <http://protege.stanford.edu>, retrieved January 3, 2008.
7. A. V. Zhdanova, R. Krummenacher, J. Henke, and D. Fensel, "Community-driven ontology management: DERI case study," in *WI '05: Proceedings of the 2005 IEEE/WIC/ACM International Conference on Web Intelligence*, (Washington, DC, USA), pp. 73–79, IEEE Computer Society, 2005.
8. B. C. Grau, I. Horrocks, Y. Kazakov, and U. Sattler, "Just the right amount: extracting modules from ontologies," in *WWW '07: Proceedings of the 16th international conference on World Wide Web*, (New York, NY, USA), pp. 717–726, ACM, 2007.
9. S. Ghilardi, C. Lutz, and F. Wolter, "Did I damage my ontology? a case for conservative extensions in description logics," in *Proceedings of the Tenth International Conference on Principles of Knowledge Representation and Reasoning (KR'06)* (P. Doherty, J. Mylopoulos, and C. Welty, eds.), pp. 187–197, AAAI Press, 2006.
10. M. Džbor, A. Kubias, L. Gridinoc, A. Lopez-Cima, and C. B. Aranda, "The role of access rights in ontology customization," Deliverable 4.4.1, NeOn Project, 2007.
11. G. Qi, P. Haase, and S. Pinto, "Context representation formalism," Deliverable 3.1.2, NeOn Project, 2007.
12. S. Kaushik, D. Wijesekera, and P. Ammann, "Policy-based dissemination of partial web-ontologies," in *SWS '05: Proceedings of the 2005 workshop on Secure web services*, (New York, NY, USA), pp. 43–52, ACM, 2005.
13. C. Farkas, A. Jain, D. Wijesekera, A. Singhal, and B. Thuraisingham, "Semantic-aware data protection in web services," in *IEEE Web Services Security Symposium (WSSS) 2006*, (Berkeley, California, USA), 5 2006.
14. S. Bechhofer, F. van Harmelen, J. Hendler, I. Horrocks, D. L. McGuinness, P. F. Patel-Schneider, and L. A. Stein, *OWL Web Ontology Language Reference*. World Wide Web Consortium, 2 2004. W3C Recommendation, available at <http://www.w3.org/TR/owl-ref/>, retrieved January 3, 2008.