# Towards Trust for Semantic Web Annotations

Wolfgang Woerndl
TU Muenchen
Boltzmannstr. 3
85748 Garching
Germany
+49 89 289 18686
woerndl@in.tum.de

## ABSTRACT

In the Semantic Web, users can attach (semantic) meta data to Web resources. One problem is the trustworthiness of these annotations. This paper identifies two main steps towards a Semantic Web trust framework and provides possible solutions.

The first step is to authenticate users and annotations. This is done in our approach by introducing Liberty Alliance identity management into Semantic Web annotations. Users have to login using Liberty Alliance accounts to create or modify annotations and their credentials are stored with the annotations. The author of an annotation can also define optional access rights to her annotations, for example to restrict access to the participants of a lecture course. We present our implementation which is an extension of the Annozilla plugin for the Mozilla Web browser. One advantage of using the Liberty Alliance specification for authentication is possible interoperability with other Web applications. Users can thereby reuse accounts for different services under their control (identity management).

The second step is a framework for expressing trust in a (Web) resource. Users can rate resources (or other trust ratings) using a trust ontology. The rating is always done with regard to a distinct facet or aspect. For example, a user can express high trust in the w3c.org Web site regarding the aspect "Web technology". Our trust ontology also integrates (optional) references to domain-specific text representations of trust values.

## Categories and Subject Descriptors

H.5.3 [**Group and Organization Interfaces**] and K.6.5 [**Security and Protection**] - Authentication

## General Terms

Design, Security, Human Factors.

## Keywords

trust, identity management, annotation, annotea, liberty alliance, authentication



## 1. INTRODUCTION

In the Semantic Web, users can attach (semantic) meta data to Web resources. These annotations can then be displayed to other users or used by computer programs to improve the understanding of content. For example, in an E-Learning scenario, users could annotate (Web) resources with meta data such as "difficult" or "important", or rate resources with regard to a certain topic or course.

One problem is the trustworthiness of annotations. In the traditional WWW, users have to manually decide whether a Web page is trustworthy or not. For example, an annotation by the lecturer of a course would constitute high trust to her students. In a Semantic Web, we need a framework for representing trust in Web resources which can be used by programs to enhance search results or information personalization, for example.

Annotea provides a standardized framework for the creation and management of annotations [1]. Usually, Web server functionality provides user authentication for annotations. Often, the standard HTTP authentication mechanism is used. In this case, users have to provide credentials to access annotations but the identity information is not associated with the annotation itself. Existing approaches for secure authentication in open networks, such as the Liberty Alliance project, are not integrated into annotation infrastructures.

In this paper, we identity two main steps towards a trust framework for (Semantic Web) annotations. First of all, we want to motivate the goal of our research by explaining an example scenario in section 2. In section 3, we describe how to authenticate users applying the Liberty Alliance standard for distributed and federated identity management (section 3). In section 4, we then explain the expression of trust in resources using a trust ontology. The paper finishes with a short discussion of related work and conclusion.

## 2. MOTIVATION AND REQUIREMENTS

Consider an E-Learning scenario, where a lecturer provides content in form of various Web pages. Users (e.g. lecturer, students, anonymous guests) could annotate and rate these E-Learning Web resources. For example, a user wants to annotate a Web page (or part of it) as "difficult" or "important" (using a Semantic Web ontology, for instance), or express her trust in the Web page. These annotations could then be used to adapt content to a learner's needs or preferences, or used by other users to evaluate resources. If annotations are written by the lecturer of the course, students certainly would have higher confidence in the reliability of the information.

Students can also make annotations but other users might find all information as completely trustworthy. In this case, it is useful to be able to express trust not only in resources such as Web pages but also in other annotations itself. If a student annotation is rated as trustworthy by several other users, this would constitute a higher level of trust.

Furthermore, when annotations are linked to user accounts, users might want to control access to their annotations. For example, a lecturer might want to restrict access to some annotations to the registered students of her course.

Requirements for trust for Semantic Web annotations can be summarized as follows:

- Securely authenticating users who want to create or manage annotations
- Associating identity information with annotations so that other users can be certain who created an annotation
- Providing means to control access to annotations
- Rating resources using trust expressions in annotations
- Expressing trust or distrust in other ratings
- Using the existing protocols such as Annotea and Liberty Alliance without much modification, if possible

These requirements roughly fall into these two categories:

1.Identity management: mechanism for securely authenticating users without necessarily relinquishing privacy considerations

2.Trust framework: an ontology and a framework for trust expressions and rating of resources

In the following two sections we will outline our ideas for a solution regarding these requirements.

# 3. INTRODUCING LIBERTY ALLIANCE IDENTITY MANAGEMENT INTO ANNOTATIONS

Our approach for identity management and user authentication is to use the standards of the Liberty Alliance project.

## 3.1 The Liberty Alliance Project

The Liberty Alliance project is an initiative by more than 150 companies and organization to provide standards for secure Web authentication (www.projectliberty.org). The Liberty Alliance specification offers a scheme to single sign on, authentication and controlled sharing of user identities among services. It uses the standard Security Assertion Markup Language (SAML) (xml.coverpages.org/saml.html) for the secure exchange of authentication information [3]. Liberty Alliance distinguishes three entities:

- principal: user, whose identity has to be verified
- service provider: the actual service the user wants to access (e.g. the annotation service)
- identity provider: a service that manages user accounts and authenticates users

In the Liberty Alliance approach, identity providers take care of the authentication of users, not the service providers. Advantages of using Liberty Alliance for Semantic Web annotations are as follows:

- Liberty Alliance provides a fully developed and proven standard for distributed authentication (this is more secure and preferable to just using HTTP authentication, for example)
- Interoperability: existing accounts can be reused for different applications, not just the annotation services
- A certain degree of anonymity remains: users do not have to provide information about their real identity, but can use a pseudonym. On the other hand, when several annotations can be securely linked to one pseudonym, a sense of trust can be achieved nevertheless

In the Liberty Alliance framework, users can manage different accounts and link them under their own control. In addition, Liberty Alliance features other privacy mechanisms, for examples regarding user consent [2].

## 3.2 Liberty Alliance and Annotea

The integration of Liberty Alliance identity management in Annotea in our approach can be outlined according to the following procedure:

1. A user wants to access a service (making an annotation) and selects an identity provider and identity (step 3 in Fig.)
2. The service provider then creates a SAML request according to the Liberty Alliance protocol and sends it to the identity provider
3. The identity provider authenticates the user (by prompting the user for a password, for example) and sends the authentication response to the service provider (annotation server/client)
4. The service provider can now analyze the response, retrieve the user name and handle the annotation protocol

In this case, the authentication process is independent from the service provider (annotation system). The advantage of this approach is that the Annotea protocol can be used without any modifications. The drawback is that user authentication information is not directly included in the Annotea protocol but has to be managed by the annotation server. This is done in our approach by using session keys to associate Annotea requests with authentication data and storing the user credentials with annotations.

Our (prototype) implementation is based on the Annozilla plugin version 0.5 beta[1] for the Mozilla resp. Firefox Web browser (annozilla.mozdev.org). Annozilla 0.5 uses JavaScript components for the annotation functionality. The main task for the implementation is to adapt the nsRemoteAnnotationService.js script for the interaction with the identity provider. For the Liberty Alliance part, we use the SourceID Open Source implementation of the Liberty Alliance specifications

[1] The current version is 0.6.6 (july 2006)

(www.sourceid.org). We also use SourceID to provide the identity provider system.

## 3.3 User Interface

Fig. 1 displays our user interface for creating an annotation. In the top part, the user can enter the text of her annotation. Then she has to select an annotation service. Depending on the service, one or more identity providers are available. In step 3 the user can select one identity provider and login using a Liberty Alliance account (as explained above). When creating several annotations within one session, the user has to login only once. Note that users cannot fill in a "author" field, because the author information is provided through the Liberty Alliance account. In step 4, the user can choose from several (facultative) options. She can select a type of the annotation, the language and a privacy attribute for the annotation.

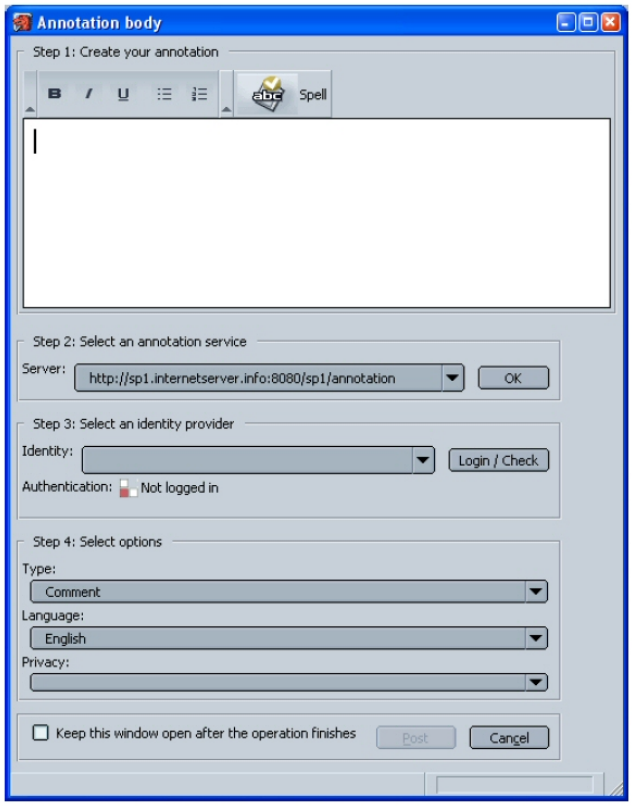


**Figure 1. Creating an annotation**

The privacy option is used to define access rights to the annotations. Because users might not want to specify detailed access rights themselves, profiles with predefined options can be provided in our framework. A simple profile might include the following options:

- public: (read) access for everybody
- private: read access only for the author of the annotation
- anonymous: everybody can read the content of the annotation, but the author information is not shown

The third option is interesting, because users have to login to create annotations in our framework and cannot make anonymous annotations by omitting author information or entering fake data.

# 4. EXPRESSING TRUST IN WEB RESOURCES

## 4.1 Overview

In chapter 3, we explained how to integrate identity management into Semantic Web annotations to securely authenticating users. The second part now is to provide a framework for expressing trust in Web resources. The idea is that users can rate Web resources. Rating thereby means assigning a trust value to a resource. These ratings (or trust statements) are stored and managed using the Annotea protocol. Our approach is not only designed to rate Web resources but also other trust expressions themselves.

All trust statements are made with regard to a distinct facet or aspect. For example, a user might find the Web site of the World Wide Web Consortium trustworthy regarding "Web technology". Since users have to login (as explained in section 3) to create trust statements, the ratings are associated with the user identity. Other examples for aspects are "design" or "function" when rating a product.

## 4.2 Trust Ontology

The core of the approach is a trust ontology that formalizes the mentioned trust statements. Fig. 2 shows an example of an instance of the ontology.

```
<rdf:RDF
... namespace definitions omitted ..>
<tr:TrustStatement
rdf:about="http://annotest.w3.org/annotations/annotation/5930134703.359235"
a:context="http://www.dgk.org/#xpointer(/html[1])"
a:created="2005-10-19T10:10:00">
<dc:creator>Werner Jansen</dc:creator>
<dc:date>2005-10-19T10:10:00</dc:date>
<a:annotates rdf:resource="http://www.dgk.org/"/>
<tr:trustRegarding>cardiology</tr:trustRegarding>
<tr:trustValue>1.0</tr:trustValue>
<tr:trustOntology
rdf:resource="http://www11.in.tum.de/sw/trust/trustOnt#"/>
<tr:trustRepresentation
rdf:resource="http:www11.in.tum.de/sw/trust/trustOnt#AbsoluteTrust"/>
</tr:TrustStatement>
</rdf:RDF>
```

**Figure 2. Trust ontology example**

The ontology consists of trust statements, with the following parts (tags highlighted in bold in Fig. 2):

- trustRegarding: this is the facet on which the trust statement is based on

- trustValue: a numerical value ranging from -1.0 (absolute distrust) to 1.0 (complete trust). 0 is neutral, i.e. “don’t know whether resource is trustworthy or not”
- (optional) trustOntology: reference to domain-specific ontology that explains the meaning of trustValues in natural language
- (optional) trustRepresentation: a specific trust value in the trustOntology

The trustOntology and trustRepresentation can be used to specify what a certain trust value really means in a given domain. This information can then be used to adapt the user interface. In this case, different values of trustRepresentation can be defined in the trustOntology, in different languages, and shown to the user when displaying annotations.

As an example in the E-Learning scenario from section 2, trustRegarding might be “relevance for exam”, the trustOntology could be various degrees of relevance, such as “very relevant” or “not really relevant, but might help”. The lecturer can then annotate material with trust statements, and, since the identity of users is securely authenticated, students can take these annotations for granted. On the other hand, students can create annotations themselves which might then be rated by other students.

The trust statements are integrated into Annotea using a distinct annotation type. Annotea uses sub classes of a class “Annotation” to describe the type of an annotation [1], for example “Comment” or “See Also”. The idea is to define a new annotation type “Trust” to represent the trust statements. These statements can then be displayed to users like normal Annotea annotations, or used to personalize information access. For example, important E-Learning material can be highlighted or Web searches of annotated pages could be ranked according to available trust statements.

## 4.3 Related Work

A lot of work is done in the field of trust for the Semantic Web. An overview gives the (slightly outdated) Semantic Web Trust and Security Resource Guide: www.wiwiss.fu-berlin.de/suhl/bizer/SWTSGuide/

Our trust ontology is similar to the one used by Golbeck, Parsia and Hendler in [4]. This approach uses FOAF (friend-of-a-friend, [5]) to identify users and built social networks. One extension is the reference to an external, domain-specific trust ontology in our model.

C.Görn recently proposed an ontology for trust models [6]. The ontology includes attributes for start and end dates of trust statements. The approach – and some other trust formalizations, including [4] – is more geared towards expressing trust in persons, not Web pages or annotations.

# 5. CONCLUSION

In this paper, we have presented an approach to improve trust for (Semantic Web) annotations. First, we have applied Liberty Alliance identity management to authenticate users. Then, we have shown how users can make trust expression by using a trust ontology.

The rating of Web resources is already done by online shops such as amazon.com, for example. With a general Web trust framework, users could rate products or other resources across different sites. Such an approach would be susceptible to spam or fake ratings. In this case, secure authentication of users is especially important. This raises privacy issues. One solution is to disallow anonymous annotations but optionally leaving out author information when displaying annotations. In our framework, this is possible by associating access rights to annotations. Trust ratings could also be used to compute similarities between users and recommend item based on this user similarity (collaborative filtering). Thereby, the explicit representation of distrust in our model is beneficial.

An idea for improvement in our approach is the introduction of aging of trust annotations. Old ratings might constitute a lesser meaning than new ratings. Another (related) problem is how to handle changes in Web resources. If a Web page is modified, the associated trust statements have to be modified as well. Future work also includes the refinement of our implementation, which include the integration in current Annozilla versions, and the application and evaluation of the approach in the E-Learning scenario.

# 6. ACKNOWLEDGMENTS

The author would like to thank his diploma/master students Markus Geiger and Werner Jansen, who worked out the details and designed and partly implemented the two parts of the system, and also Manuel Giuliani, who worked on the demo application.

# 7. REFERENCES

[1] Kahan, J., Koivunen, M., Prud'Hommeaux, E. and Swick, R. Annotea: An Open RDF Infrastructure for Shared Web Annotations. In *Proc. of the WWW10 International Conference*, Hong Kong, May 2001.

[2] Liberty Alliance Project Whitepaper: Personal Identity. http://www.projectliberty.org/resources/whitepapers/Personal_Identity.pdf, 2006.

[3] Watson, T. (ed.) Liberty ID-FF Architecture Overview. http://www.projectliberty.org/specs/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf

[4] Golbeck, J., Parsia, B. and Hendler, J. Trust networks on the semantic web. In *Proceedings of Cooperative Intelligent Agents (CIA)*, Helsinki, Finland, 2003

[5] Dumbill, E. XML Watch: Finding friends with XML and RDF. IBM Developer Works, http://www-106.ibm.com/developerworks/xml/library/xfoaf, 2002

[6] Görn, C. An extended Ontology for Trust Models. http://b4mad.net/2006/01/10/trust.html