MyID

Decentralized User Profile and Identity on the Web

Andrei Sambra, Maryline Laurent

TELECOM SudParis
CNRS Samovar UMR 5157
9 rue Charles Fourier, 91011 Evry, France.

Abstract

MyID intends to provide a solution for managing the numerous accounts and profiles that users have on the Internet. Its main purpose is to provide a unified user account, or simply 'user profile' , which as opposed to current 'silo' profiles, would really be under the user's control. All of this can take place now, using technologies already available to the users. This paper addresses the technical aspects involved in providing such a unified user profile, taking into consideration the emerging privacy issues.

Keywords: semantic web, linked data, decentralized profiles, online identity, public key cryptography

1. Current Issues

The Web we know is based on centralized resources, the so called 'silo' approach. Offering particular services would usually involve having to create dedicated accounts for each user, tying and limiting the user to this particular service and/or resource. Furthermore, users have no control over how their personal account data are used by the service. Recently there have been numerous cases where social networks have made public certain private details of their users (see Facebook and Google Buzz), which made people realize the importance of online privacy and public data control.

One may argue that better privacy policies may reduce the risk of exposure. However, even if users decide to protect their public data or even remove their accounts, there is no guarantee that the process is instant and permanent, since most of the countries have passed laws which require that online data be stored for several months up to one year or

more.

Another important issue deals with authentication and identification. Most of the services authenticate users based on username and password combinations. Federated and single sign-on services like OpenID have proven to be quite useful. However, implementing a cross-domain authentication and user management system not only requires a lot of effort from large entities in order to make everything compatible, but also powerful trust relationships. In addition, once authentication has been performed, services still require that users have local profiles.

To put things into perspective, let's take the case of Facebook. Its success attracts more and more people to use it, encouraging its developers to provide even more services. When these services prove useful, users start to depend on them on a daily basis. There have been people recently discussing the possibility of having Facebook act as a bank, or as an intermediary (PayPal). What if something happens tomorrow and the all services offered by Facebook suddenly become inaccessible? What happens to all the time and data we have so carefully invested into developing a rich user profile?

2. MyID

This is where MyID comes into play. The proposed solution addresses the shortcomings of the silo-based user accounts, cross-domain authentication and identification, as well as data sharing and propagation.

2.1 Authentication and Identification

In order to perform authentication and identification, MyID is based on the recent standard proposed by W3C's WebID[1] Incubator Group, and the *Friend of a Friend* (FOAF)[2] ontology.

WebID proposes a way to uniquely identify a person, company, organization, or other agents, using a URI which is included in an X.509 browser certificate. The authentication process relies on TLS to validate that the private key in use matches the public key of the declared certificate, as well as the public key found in the profile at the location indicated by the URI. In other words, it provides a cryptographic way of authenticating and identifying a user, based on resources managed by the user -- the browser certificate and the corresponding profile accessible at the URI location.

The FOAF project is creating a Web of machine-readable pages describing people, the links between them and the things they create and do; it is a contribution to the linked information system known as the Web[3]. FOAF defines an open, decentralized technology for connecting social Web sites, and the people they describe.

Combining WebID and FOAF offer users the possibility to directly participate in their interactions across the Web, by allowing them to use a unique identity (pointing to a unique user account / profile), across multiple domains and services. This approach comes in

contrast to current practices, where the Web centralizes all our personal data through the multitude of online forms we have to fill in, instead of allowing users to carefully select which information they want to make public when accessing a particular service.

2.2 User Profile

A typical user profile will be an RDF file, initially containing a reference to the main topic of the profile (i.e. a *Person* type of resource describing the user to which it belongs), followed by the actual profile data, described using the FOAF ontology[4]. In addition, it must also contain at least a public key belonging to an X.509 browser certificate. A simple representation of a profile is provided in Figure 1.

Depending on the user's social interactions on the Web, the profile could also contain resources like blog and forum posts, or even mailing list messages, all described using the Semantically-Interlinked Online Communities (SIOC)[5] ontology.

The *Description of a Project* (DOAP)[6] and *Bug And Enhancement Tracking LanguagE* (Baetle)[7] ontologies can be used to describe project data and bug tracking information belonging to a user.

Users can also provide a list of interests, which can then be used to build and offer personalized recommendation services, thus eliminating the need for profile tracking or complex recommendation algorithms.

Still, probably the most important advantage is that all the modifications performed on a profile are instantly available to everyone making a request for the user's data. In other words, our friends or even other services will have access to the new data as soon as they become available.

2.3 Putting Everything Together

Since all the relying technologies already exist, we would like to propose a system that would combine these technologies to provide a user-friendly service, running on the user's computer, or a device belonging to the user -- possibly a plug computer, with access under the user's control.

This system can be installed on a web server, allowing read access to the profile file. It must be able to present the user with an HTML form allowing him to create an extensive profile, as well as an X.509 browser certificate. It should also allow the user to modify his/her profile in a dynamic RESTful way, while at the same time it should protect the user's privacy by being able to enforce different access rules for each profile element (resource).

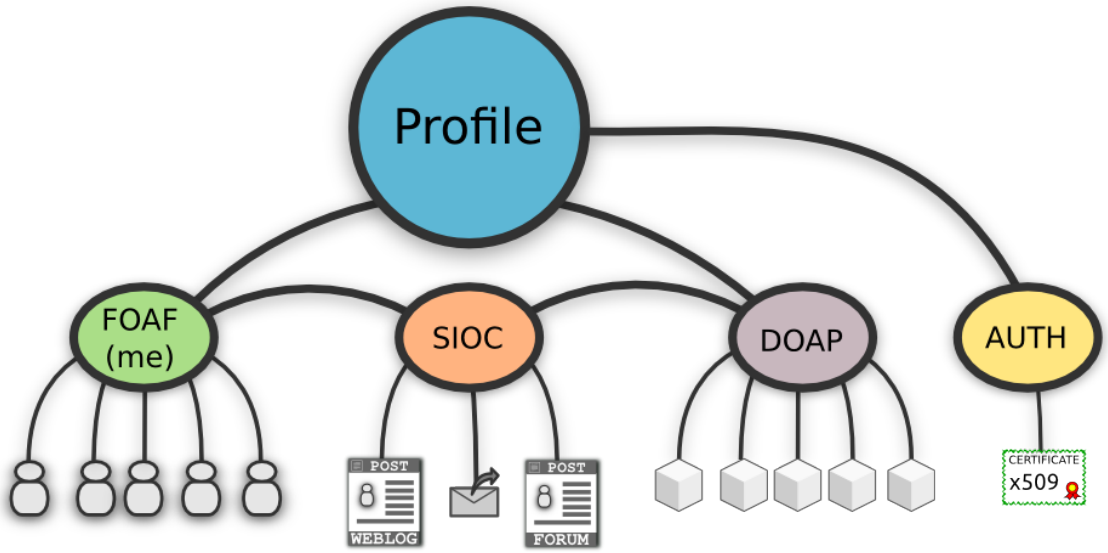

Figure 1. A typical MyID profile document.

MyID transforms a simple FOAF profile in a true online identity, aiming to offer authentication and privacy control to its users, as well as the possibility to build services which take advantage of the user's semantic profile. Such services could provide news aggregation (RSS reader), shopping recommendations, music recommendations, and even social networking.

For example, a news aggregation system could simply parse the user's profile to create a list of his feeds, and then search for additional feeds in the profiles of all the users described by existing *foaf:knows* relations. Special settings could allow the possibility of recursively building a list of feeds, which can then be filtered based on the user's *foaf:interest* entries.

An additional service could also create an RSS feed displaying all the modifications performed by the user on his/her public data, alerting potential subscribers to the changes taking place. Think of it as the status updates currently offered by social networking services.

Access to resources can be managed by a 'policy enforcer', an abstraction layer between access requests and profile contents. This layer can be based on semantic ACLs, which would follow a RESTful access system. The final ontology on which the ACLs will be based is still under review, since we still need to consider all the use cases. More information will be provided in the next section.

Once the proper access rules have been configured, services can be also be allowed to interact with user profiles in a RESTful way. For example, updating the user's list of interests when the user performs a special action -- clicking on a button labeled '*Add interest*'. Of course, special attention will be given to all the security aspects involved in implementing such a feature.

3. Future Development

Right now we are getting very close to finishing a prototype for such a system. However, the most important issue we must consider when dealing with public profiles is to assure privacy, and if possible anonymity.

Privacy in the Semantic Web is still a new topic and for this reason we were unable to find viable proposals, offering access control. We are currently working together with the W3C WebID Incubator Group, in an attempt to provide a solution to this issue as quickly as possible, while at the same time avoiding to introduce an additional layer of complexity to existing technologies.

It is imperative that the user be allowed to choose the level of privacy he/she desires, independently of the type of resource he/she intends to protect. User privacy is and will remain our foremost goal while implementing MyID.

To stay up to date with our latest progress, you can subscribe to the project's RSS feed[8].

4. Conclusions

In this position paper, we tried to emphasize the advantages of switching from a silo-based user account (profile) system to a decentralized user-controlled one. Not only would this system provide better control of a user's online identity, but it would facilitate and improve the way in which we currently experience the Web.

5. References

[1] http://www.w3.org/wiki/WebID
[2] http://www.foaf-project.org/
[3] http://www.w3.org/History/1989/proposal.html
[4] http://xmlns.com/foaf/spec/
[5] http://sioc-project.org/ontology
[6] http://trac.usefulinc.com/doap
[7] http://code.google.com/p/baetle/
[8] http://myid.fcns.eu/