Open-source Identity Federation with Shibboleth

(submission to EUNIS'2006 for a long paper)

Pascal Aubry

IFSIC / University of Rennes 1, France

pascal.aubry@univ-rennes1.fr

Extended abstract

Single Sign-On is widely deployed in the French Education/Research community, especially CAS [1]. In addition to improving the security, it allows users to authenticate once and use several web applications, as long as the applications are proposed by their institution.

New projects in France now encourage the cooperation between universities, making them share web resources (documents and applications). In the first part, we list these new usages:

- Opening local web resources to the members of other institutions,
- Manage an intranet for a geographically distributed population,
- Inside an establishment, extend SSO features to the propagation of user attributes,
- Manage the authentication of users at the frontier of institutions (ancient or future students for instance),
- From the portal of an institution, read electronic publications proposed by commercial partners.

We show that Single Sign-On technologies are not sufficient to handle these new needs, and that multiplying the authentication databases is very time-consuming and obviously not scalable (cf figure 1).

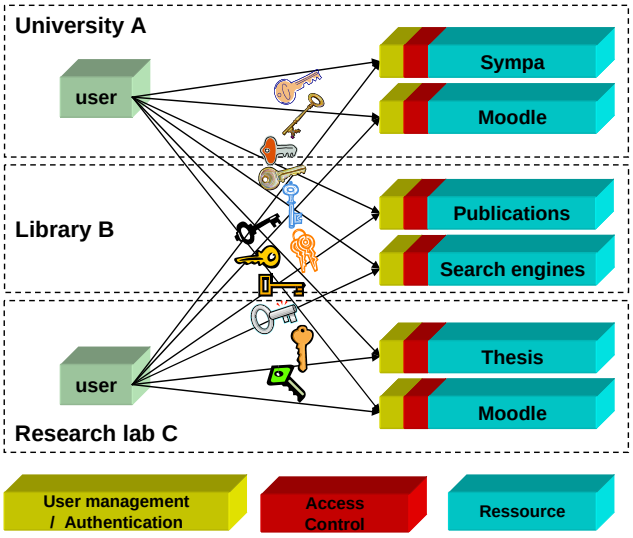

Figure 1 – Sharing web resources without Identity Federation (inspired by SwithAAI)

The step beyond Single Sign-On at establishment-level is Identity Federation, at country-level (or wider). It provides (cf figure 2):

- Comfort for the users, since Single Sign-On is extended to give access to resources outside of their institution;
- Security and scalability for the administrators, as user management is now done locally, while access control is still done at resource-level.

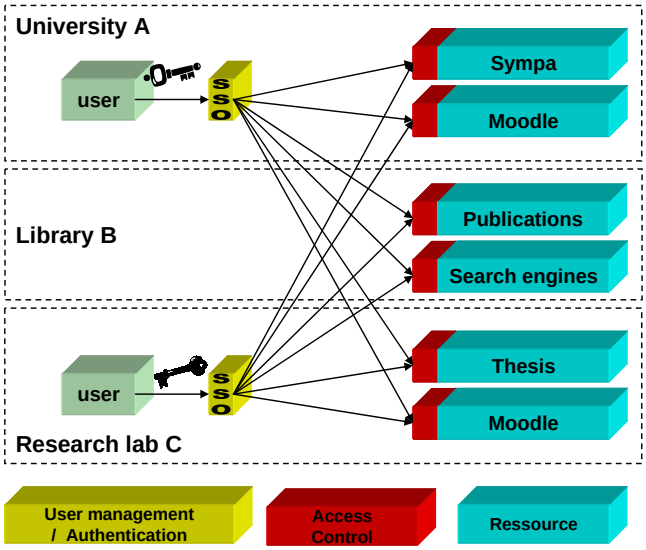

Figure 2 – Sharing web resources with Identity Federation (inspired by Switch AAI)

We briefly present the formats, standards and implementations that are candidate technologies for Identity Federation (cf figure 3), especially SAML (Security Assertion Markup Language [2]), the XML standard adopted by Liberty Alliance [3] and Shibboleth [4].

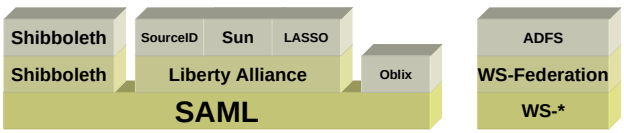

Figure 3 – Technologies for Identity Federation

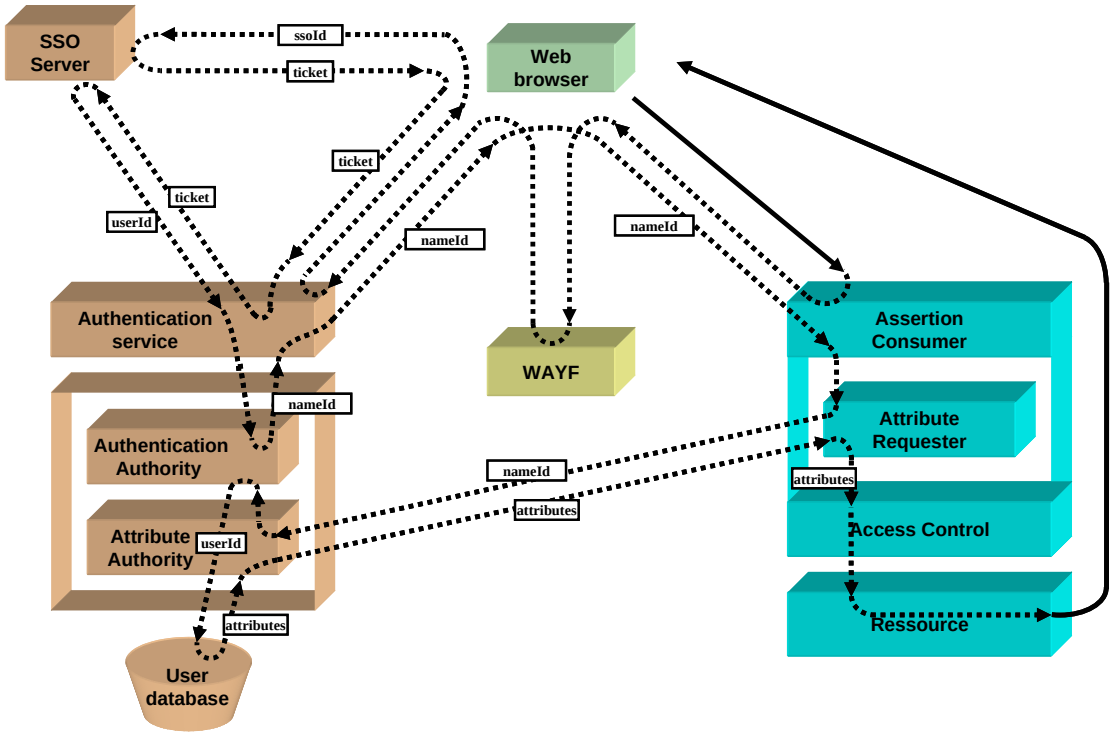

Figure 4 – The cinematic of Shibboleth

In France, these technologies have been evaluated by CRU[1]; we explain the reason that made them choose Shibboleth to implement their federation [5] (at country-level).

Understanding the architecture of a complete Shibboleth deployment is not easy, since there are many actors, protocols and interactions (cf figure 4).

The last part of the paper:

Describes the actors of the system,

Fully explains the cinematic of Shibboleth.

The goal of the article is to demystify Shibboleth, as the solution (and concurrent solutions as well) is often considered an opaque and delicate architecture. We introduce the architecture progressively, by adding some complexity at each stage:

1. A user requests a Service Provider (SP), using a simple identity provider (IdP).
2. The Service Provider relies on a SSO server.
3. An additional actor named WAYF[2] allows users to select their institution among the members of a federation.

At each stage, we clearly explain the interactions, step by step.

To conclude the article, we discuss the WAYF (localization in a federation, ergonomic aspects), point out a few issues encountered when setting up a federation, and present some work perspectives (virtual Identity Provider, n-tiers installations…).

References

[1] Pascal Aubry, Vincent Mathieu and Julien Marchal, Open-source Single Sign-On with CAS (Central Authentication Service). In Actes of EUNIS'2004, Bled, Slovenia, July 2004, best paper award, published in the journal Uporabna informatika (Applied Informatics, ISSN 1318-1882, surveyed by INSPEC), ed. Prof. Andrej Kovacic.

[2] *OASIS Security Services (SAML)*, www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

[3] The Liberty Alliance Project, www.projectliberty.org.

[4] *The Shibboleth Project*, shibboleth.internet2.edu.

[5] The CRU federation, federation.cru.fr.

The author

Pascal Aubry manages web-projects at University of Rennes 1. He has been part of the ESUP-Portail project since its inception in late 2002, notably working on web security (SSO, authorizations).

[1] CRU stand in French for "Network Committee for Universities".

[2] WAYF stands for "Where Are You From".