AAI: Autenticazione federata e biblioteche digitali

Domenico Dellisanti
CILEA, Segrate

Abstract
Questo articolo presenta la descrizione di un esempio di funzionamento del sistema Shibboleth mettendo in risalto come avviene lo scambio delle informazioni tra le varie componenti dello stesso sistema. Inoltre è presentato un primo esempio di federazione relativa alle biblioteche digitali, con l'illustrazione delle principali implicazioni che l'applicazione di una federazione ha sulle biblioteche e sugli editori fornitori dei servizi di editoria elettronica.

This article presents the description of an example of how the Shibboleth system works, underlining how the information is exchanged between the components of the system. Moreover, it describes a first example of a federation of digital libraries and it illustrates the main implications of the application of a federation on libraries and publishers that provide electronic publishing services.

Keywords: Authentication, Authorization, Consortium, Digital Library, Shibboleth, Federation.

La II giornata dedicata all'Authentication & Authorization Infrastructure (AAI) [1] (Autenticazione federata e biblioteche digitali), che si è svolta a Roma in data 6 marzo 2007, è stata preceduta da un seminario teorico-pratico di introduzione a Shibboleth [2]. Il seminario, tenuto da Giacomo Tenaglia del CNR – Biblioteca d'Area di Bologna, ha presentato l'architettura e il funzionamento di Shibboleth e ha illustrato i passi necessari per l'installazione delle sue componenti.

Shibboleth è un software middleware open source, basato sullo standard Security Assertion Markup Language (SAML) [3], che fornisce un Single Sign On (SSO) sul Web all'interno di un'organizzazione o tra organizzazioni diverse. Permette a siti e servizi Web di autorizzare o meno l'accesso a risorse online protette. Questo articolo riguarda in particolare l'applicazione della AAI e di Shibboleth al settore delle biblioteche digitali. Per una descrizione completa di Shibboleth, si veda l'articolo "Il CILEA collabora alla creazione della Federazione AAI italiana", in questo stesso numero del Bollettino CILEA.

Esempio di funzionamento di Shibboleth

La figura 1 mostra un esempio di funzionamento di Shibboleth, in cui l'utente cerca di accedere al servizio a cui crede di avere i diritti di accesso; supponiamo che cerchi di accedere alle riviste pubblicate da ACS Publications. Il server ACS, che nel nostro contesto costituisce il *Service Provider* (SP), non accetta la richiesta e la inoltra al *Where Are You From* (WAYF) [4], che ha il compito di decifrare chi è l'utente in questione. A questo punto, dietro richiesta da parte del WAYF, l'utente fornisce allo stesso WAYF le informazioni che lo identificano e questo ultimo chiede al *Handle Service* del *Identity Provider* (IdP), ossia l'organizzazione a cui l'utente ha dichiarato di appartenere, una conferma. Il Handle Service è uno dei componenti del Identity Provider, che rappresenta appunto l'istituzione. Questo stesso richiede all'utente di non accedere direttamente sul sito remoto dell'editore ACS, ma di utilizzare il Web Login, ossia di accedere tramite Shibboleth, al fine di essere riconosciuto e conseguentemente di accedere in maniera automatica a qualsiasi risorsa a cui ha diritto. L'utente viene riconosciuto grazie al confronto dei dati personali contenuti nel database degli utenti (User DB). Tramite il Handle di Shibboleth, le credenziali dell'utente vengono passate al Service Provider, ossia ad ACS, fase 8, che valida l'utente e l'asserzione. Ma al Service Provider mancano ancora gli

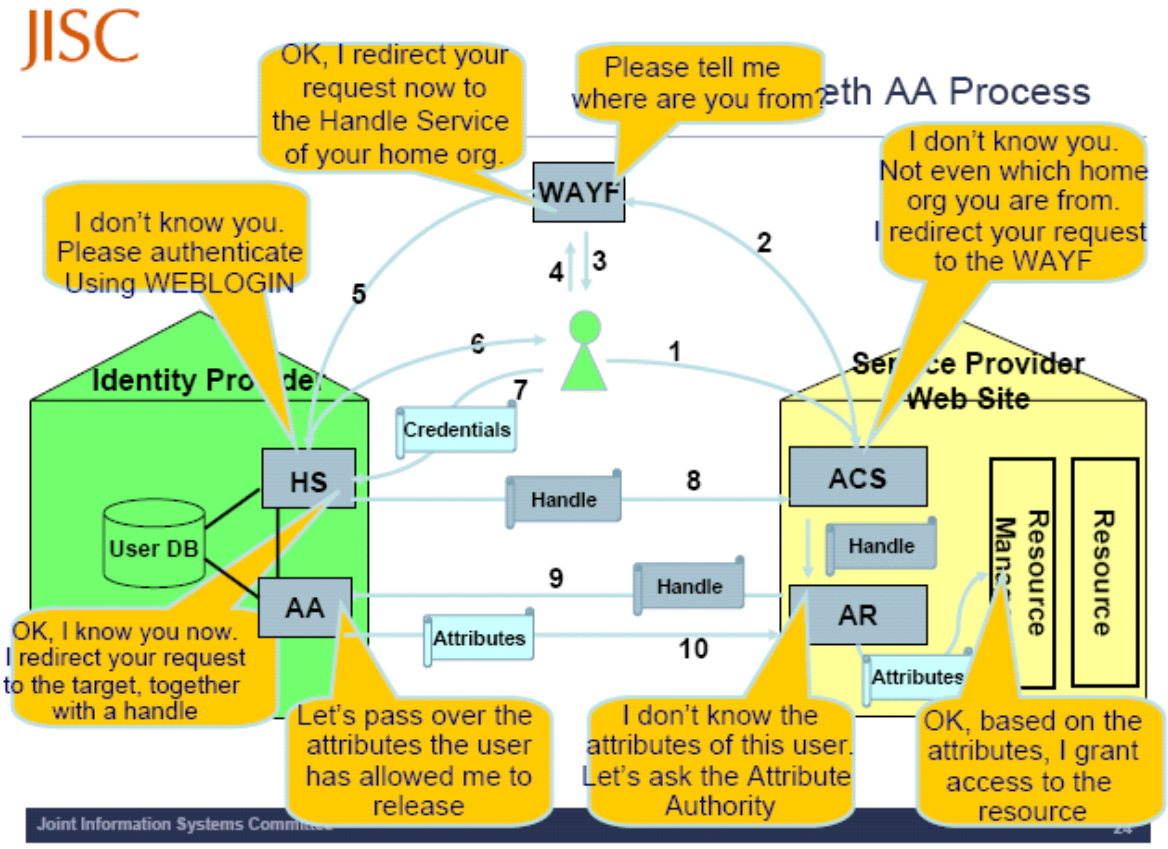

Fig. 1 - Esempio di funzionamento

attributi dell'utente, ossia essi non sono stati ancora registrati nel *Attribute Resource* (AR). Quindi si rende necessaria una nuova richiesta verso l'IdP, al fine di recuperare i dati relativi agli attributi dell'utente attingendo al *Attribute Authority* (AA). L'IdP riconosce il Service Provider che ha inoltrato la richiesta, lo valida e stabilisce quali attributi sia necessario trasmettergli. Questi vengono inviati al fine di ultimare la fase di autorizzazione e permettere così all'utente di accedere alla risorsa da lui richiesta.

Inoltre, in questo modo l'utente ora è stato riconosciuto, i suoi dati memorizzati e, quindi, può accedere a qualsiasi altra risorsa o servizio di cui possiede i diritti di accesso.

Il fatto innovativo è che non ci sono nuovi username o password da ricordare o distribuire con il timore di perderli.

Per poter accedere a ciò a cui si ha diritto è sufficiente autenticarsi tramite il Web Login, che permette all'utente di essere riconosciuto da qualsiasi posto cerchi di connettersi, superando in questo modo i limiti fisici legati al riconoscimento degli IP, che spesso inibisce gli utilizzatori che in quel particolare istante non sono presenti all'interno della rete dell'ente di appartenenza.

È a disposizione degli utilizzatori un help online, che facilita l'uso dello strumento in questione, di cui non è necessario assolutamente conoscere i particolari dell'architettura per poterlo correttamente utilizzare.

Affinché tutto questo sia veramente applicabile e dia i risultati voluti, è però necessario che le organizzazioni stesse creino delle superstrutture di condivisione dei dati di autenticazione dei loro utenti, le cosiddette federazioni.

Federazione in Gran Bretagna

John Pashoud, afferente al Joint Information Systems Committee (JISC) [5], nel suo intervento: "What Universities need to do about Access Management, and what Britain is doing about it", ha illustrato la realtà inglese, in particolare quella della LSE Library, ossia London School of Economics & Political Science [6].

La LSE è un raggruppamento di università specializzate nel campo delle scienze sociali, caratterizzato dal fatto che frequentemente gli studenti e il personale afferente lavorano fuori dal campus, ma hanno bisogno di accedere a tutti i servizi e le fonti di informazioni a cui hanno diritto in quanto affiliati alla stessa LSE.

La biblioteca, rinomata in tutto il mondo nel campo delle scienze sociali, è solitamente frequentata da ricercatori provenienti da altre università e da varie istituzioni appartenenti anche alla sfera governativa. Si è reso quindi necessario implementare e mettere in funzione un sistema che permettesse a tutto il personale di accedere a qualsiasi risorsa, senza la necessità di dover ricordare le differenti password per ciascun servizio utilizzato, da qualsiasi posto fisico e assicurando la riservatezza dei dati personali. Il costo che una scelta del genere comporta è principalmente quello di supportare un Shibboleth Identity Provider, oltre all'istallazione e alla manutenzione dello stesso.

I benefici che si traggono sono molteplici:

- credenziali uniche dell'utente, abbandonando la necessità di memorizzare password diverse per ciascun servizio;
- nessuna differenza di accesso dal luogo istituzionale e da una qualsiasi altra postazione;
- maggiore flessibilità nel controllo degli accessi, con la possibilità di creare categorie distinte di utenti a livelli differenziati a secondo della tipologia di servizi;
- il tempo per il controllo degli accessi ai servizi interni è completamente trascurabile.

Si può facilmente notare come i benefici superino di gran lunga i costi.

Nel suo intervento, Paschoud ha anche illustrato come la situazione in Inghilterra si è evoluta in questi ultimi anni. Si è partiti dal sistema già esistente, Athens [7], per poi passare a Shibboleth, ideato da Eduserv [8]. Al momento, hanno aderito all'iniziativa 641 istituzioni, tramite BECTA (British Educational Communications and Technology Agency), e circa 30.000 scuole, attraverso degli Identity Provider virtuali dislocati nelle varie regioni.

Ciò a cui si mira è una federazione di istituzioni basate su Shibboleth [9] o, meglio, una federazione di federazioni, in quanto sono già state costituite federazioni di diversa natura.

In Inghilterra è presente la UK Access Management Federation [10], che si è costituita ufficialmente in data 30 novembre 2006, costruita sul successo della federazione pilota SDSS, che era presente sul territorio inglese sin dal marzo del 2004. Il ruolo principale della federazione è quello di gestire le relazioni tra gli Identity Provider e i Service Provider. Inoltre, la stessa federazione svolge i seguenti compiti:

- valida i nuovi enti che intendono aderire;
- gestisce la lista di tutti i partecipanti;
- mette a disposizione il servizio WAYF;
- aderisce agli standard tecnici tradizionali;
- assicura una politica di controllo;
- fornisce supporto e consigli.

L'obiettivo a cui si mira è quello di costituire una federazione che possa raccogliere in sé tutte le istituzioni che intendono aderire a Shibboleth. I costi sarebbero dati dallo sforzo istituzionale di implementare il software, aderire alla federazione e aumentare i direttori istituzionali. I benefici si tramuterebbero nel pieno controllo delle istituzioni, in uno staff altamente professionale e nella gestione degli accessi per qualsiasi tipo di risorsa sia essa interna o esterna.

La UK Access Management Federation, oltre alle informazioni che fornisce sul proprio sito e a un servizio di help-desk, è ben lieta di mettere a disposizione di chi fosse interessato tutte le informazioni possibili tramite due mailing list:
jisc-shibboleth-announce@jiscmail.ac.uk
jisc-shibboleth@jiscmail.ac.uk

Ma, come anche esplicitamente annunciato da Paschoud, il percorso da compiere è ancora lungo e restano da raggiungere molti obiettivi. Infatti, si sta cercando di migliorare la presentazione delle guide all'uso, affinché gli utenti possano facilmente comprendere il funzionamento del sistema e garantire dei livelli di sicurezza a seconda delle risorse che si stanno prendendo in esame.

Da parte degli editori

Un servizio di editoria elettronica può non essere necessariamente configurato come Service Provider, ma può identificare un qualsiasi altro servizio, per esempio di e-learning, a cui è possibile accedere tramite autorizzazione. Questa scelta si sta sempre più diffondendo e, di conseguenza, sono diversi gli editori o *information provider* che hanno implementato Shibboleth sui loro server (Elsevier, Ex-Libris, CSA, JSTOR, EBSCO, DSpace).

Karen Grove, di Ex-Libris, nel suo intervento, ha illustrato la scelta che ha compiuto la propria azienda con l'adozione del modulo PDS, ossia Patron Directory Service. Questo permette l'esistenza di un unico punto di integrazione con i sistemi di autenticazione dei vari prodotti Ex-

Libris, semplifica di molto la gestione amministrativa, fornisce un Single Sign On (SSO), viene incontro alle esigenze consortili nel caso in cui ciascuna istituzione facente parte dello stesso abbia un proprio sistema di autenticazione e un database di attributi, è compatibile con Shibboleth.

Scenari futuri

Per il futuro si pensa alla possibilità che possano coesistere diverse soluzioni tutte però aventi lo stesso fine. Come lingua franca la scelta non può che ricadere su SAML, in particolare ricorrendo alla versione 2.0 e alla creazione di una federazione di federazioni.

La prima confederazione europea è eduroam [14], che ha il compito di gestire la rete per gli accessi alle istituzioni che ne fanno parte.

Quindi, si può concludere affermando che non ci sarà un'unica federazione che ingloberà tutte le altre, ma l'obiettivo che si vuole raggiungere è quello di arrivare appunto a diverse federazioni che cooperano tra loro.

Bibliografia

[1] Sito di AAI
URL: http://www.switch.ch/aai/docs/AAI-Flyer_en.pdf
[2] Sito di Shibboleth Project
URL: http://shibboleth.internet2.edu/about.html
[3] Sito Standard SAML
URL: http://www.oasis-open.org/committes/security
[4] SWITCH WAYF
URL: http://www.switch.ch/aai/wayf
[5] Sito di JISC
URL: http://www.jisc.ac.uk/whatwedo/themes/access_management.aspx
[6] Sito della LSE library
URL: http://library.lse.ac.uk
[7] Sito di Athens
URL: http://www.athens.ac.uk/
[8] Sito della Eduserv
URL: http://www.eduserv.org.uk/
[9] Federazioni basate su Shibboleth:
URL: https://spaces.internet2.edu/display/SHIB/ShibbolethFederations
[10] Sito della UK Access Management Federation
URL :http://www.ukfederation.org.uk/