

Il CILEA entra nella Federazione IDEM del GARR

Roberto Gibellini

CILEA, Segrate

Abstract

Con l'attivazione di un Identity Provider Shibboleth il CILEA entra a pieno titolo a far parte del progetto pilota IDEM (IDentity Management) per la realizzazione dell'Infrastruttura di Autenticazione e Autorizzazione federata della rete GARR.

This article presents a new project CILEA is now involved into: joining an initiative by the GARR Consortium, we realized a Shibboleth Identity Provider so we are now in the IDEM (IDentity Management) project working on the creation of an Italian Federation of AAI (Authentication and Authorisation Infrastructure).

Keywords: IDEM, AAI Federation, Shibboleth, Single Sign On.

Introduzione

Gli ultimi anni hanno visto il proliferare di numerosi servizi web ognuno con un differente sistema di autenticazione.

Partendo dalla tradizionale autenticazione con userid/passwd (figura 1) fino ad arrivare ai più recenti sistemi basati su smartcard e certificati personali, l'accesso alle informazioni è generalmente regolato da una serie di "iscrizioni" che richiedono ad ogni singolo utente di fornire di volta in volta differenti credenziali. Considerando inoltre che tali identità digitali implicano spesso il passaggio nella rete di dati personali soggetti a regole di sicurezza e riservatezza diverse, si capisce fin da subito come questa modalità renda difficile e insicuro l'accesso a servizi online forniti da soggetti diversi dalla propria "organizzazione di appartenenza".

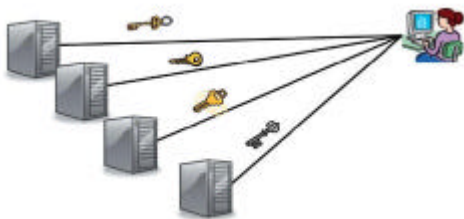


Fig. 1 – Autenticazione tradizionale

In tale ambito il Consortium GARR [1], come già hanno fatto enti omologhi (quali Switch [2] in Svizzera, RedIRIS [3] in Spagna, Uninett [4] in Norvegia, ecc.), intende favorire e supportare l'attivazione di una Federazione dei sistemi di autenticazione degli Atenei e Enti di Ricerca (qui di seguito chiamata Federazione GARR-AAI), basata su rapporti di reciproca fiducia, all'interno della quale sia accettata l'identità digitale dell'utente riconosciuta dall'organizzazione di appartenenza. Un processo analogo, dal punto di vista logico, a quanto accade per i cittadini dei paesi membri della comunità europea che accettano la carta di identità del paese di riferimento.

AAI in pillole

Una AAI (Authentication and Authorization Infrastructure) gestisce le procedure di autenticazione e autorizzazione tra un utente, la sua organizzazione di origine e i servizi offerti sulla rete (figura 2).

Nell'ambito di un'infrastruttura di identity federata, i fornitori di servizi e le organizzazioni di appartenenza degli utenti possono scambiare informazioni sull'identity degli utenti in modo sicuro, coerente e rispettoso dei diritti di riservatezza degli utenti finali.

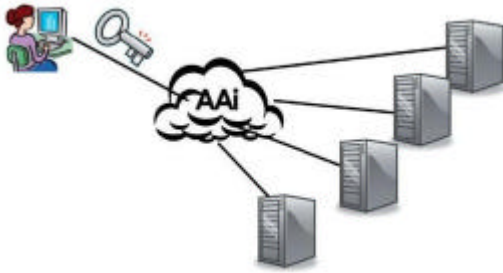


Fig. 2 – Situazione con una AAI

Ciò consentirà:

- all'utente finale di utilizzare le credenziali fornite dal proprio ente di appartenenza per l'accesso ai servizi convenzionati con la Federazione e di essere informato sui dati comunicati al fornitore di servizi in quanto necessari per l'autorizzazione e/o personalizzazione;
- all'organizzazione di appartenenza dell'utente di mantenere il controllo sul processo di autenticazione e sull'accesso ai servizi remoti da parte dei propri utenti;
- al fornitore di servizi di evitare gli oneri di gestione delle credenziali personali degli utenti e di disporre, ai fini dell'autorizzazione, di informazioni concordate con la Federazione e trasmesse a cura dell'organizzazione di appartenenza.

Il CILEA all'interno di IDEM

La prima tappa della Federazione GARR-AAI (figura 3) è stata quella di far partire un progetto pilota denominato IDEM [5], basato su tecnologia Shibboleth [6], all'interno del quale verificare l'effettiva realizzabilità di una infrastruttura di tale tipo in Italia.



Fig. 3 – Logo della Federazione

Per fare ciò il GARR promuove e supporta il progetto fornendo l'infrastruttura centrale e i servizi mettendo a disposizione:

- supporto tecnico per l'implementazione di un Identity Provider (IDP) e Service Provider (SP);
- realizzazioni di riferimento opensource;
- il servizio WAYF (Where Are You From);
- gestione della mappa della federazione.

Il CILEA è stato uno tra i primi enti ad aver attivato un Identity Provider Shibboleth conforme alle direttive della GARR-AAI e sta lavorando al fine di rendere “Shibboleth compliant” alcuni dei propri servizi per gli utenti:

- Dspace: siamo già in grado di implementare l'autenticazione via Shibboleth (prima installazione realizzata con l'Università di Parma);
- Metalib: siamo già in grado di implementare l'autenticazione via Shibboleth;
- Suite LightHouse: la configurazione è in fase di testing;
- Cilea Science Direct on Site (SDoS): la configurazione è in fase di testing.

È anche in fase di studio la possibilità di fornire un servizio di IdP per i piccoli enti che ne facessero richiesta.

Bibliografia

- [1] URL: <http://www.garr.it>
- [2] URL: <http://www.switch.ch/it/aa1>
- [3] URL: <http://www.rediris.es/index.en.html>
- [4] URL: <http://www.uninett.no/index.en.html>
- [5] URL: <http://www.idem.garr.it>
- [6] URL: <http://shibboleth.internet2.edu>