Che cos'è la Federazione IDEM e che servizio offre all'e-learning. Il ruolo del Servizio IDEM GARR AAI.

Nuove opportunità per le piattaforme e-learning

Autori: Maria Laura Mantovani, GARR e Università degli Studi di Modena e Reggio Emilia, marialaura.mantovani@garr.it, Barbara Monticini, GARR, barbara.monticini@garr.it, Simona Venuti, GARR, simona.venuti@garr.it
Parole chiave: sicurezza, identity provider, service provider, federazione IDEM, e-learning,

Le problematiche bloccanti dell'accesso tradizionale che vengono risolte dall'accesso federato

Quando ci troviamo di fronte ad un sistema, un servizio, una risorsa che ci chiede dei codici di accesso (nome utente e password, le credenziali) (Figura 1), spesso rimaniamo bloccati perché non li ricordiamo più oppure dobbiamo dedicare tempo alla ricerca del luogo dove li abbiamo riposti per non dimenticarli.

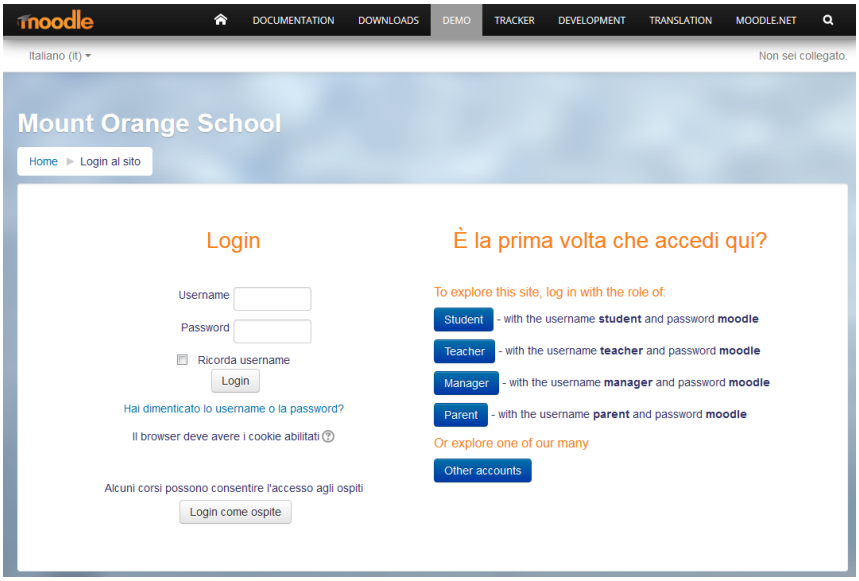


Figura 1

Ognuno di noi infatti possiede ormai molteplici codici di accesso, molteplici credenziali (Figura 2): una per la posta elettronica, una per ciascun corso on line, una per i servizi istituzionali, una per la condivisione di materiale con i nostri collaboratori, per la documentazione scientifica a pagamento, per gli ebook, per gli acquisti on-line, per i social network, ecc…



Figura 2

Tra le tante credenziali che abbiamo in dotazione, molte volte non sappiamo più quali sono quelle giuste da usare in ciascun servizio. Avere molteplici codici di accesso aumenta il rischio potenziale di furto o scambio non autorizzato d'identità.

A volte nella nostra organizzazione ci viene assegnata una credenziale che ci permette di accedere a tutte le risorse locali (Single Sign-on istituzionale). Tuttavia questa credenziale rimane una delle tante che possediamo, perché comunque abbiamo bisogno di altre credenziali per le risorse esterne alla nostra organizzazione. Se d'altra parte siamo fornitori di risorse on line, ad esempio un MOOC o semplicemente

un e-learning management system, i nostri utenti si troveranno probabilmente anche fuori dalla nostra istituzione, quindi il Single Sign-on istituzionale risulterà insufficiente.

Un altro problema che deve affrontare l'utente nella modalità tradizionale di accesso alle risorse è quella della compilazione del modulo di registrazione al servizio la prima volta che si tenta l'accesso (Figura 3). Ogni nuovo servizio on-line ci chiede tanti dati personali e solitamente sempre gli stessi. L'utente è demotivato a compiere questa operazione di registrazione soprattutto se ritiene che l'accesso alla risorsa sarà necessario solo una o poche volte. Sempre più spesso i gestori di servizi on-line notano che i nuovi utenti rinunciano all'utilizzo del servizio piuttosto che completare la procedura di registrazione. Il motivo dell'abbandono, oltre al tempo che l'utente considera perso, è anche da imputare alla preoccupazione dell'utente a rilasciare ovunque i propri dati personali.

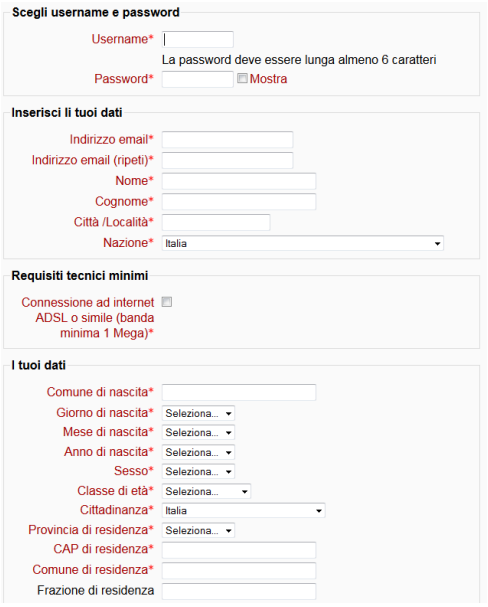


Figura 3

Anche dal punto di vista di chi offre il servizio, la gestione locale degli account crea problemi difficilmente risolvibili, quali la veridicità dei dati che l'utente introduce e l'obsolescenza a cui questi dati vanno incontro. Per affrontarli il gestore dovrebbe investire in attività di validazione e manutenzione dei dati raccolti. Inoltre la gestione locale delle credenziali utente introduce nel servizio tutte le problematiche di sicurezza nella conservazione dei relativi dati personali collegati alle credenziali e nella prevenzione e mitigazione delle vulnerabilità informatiche del servizio stesso.

La soluzione introdotta con la gestione federata delle identità e degli accessi

La gestione federata dell'identità introduce una grande novità e un nuovo paradigma, infatti permette di superare le problematiche connesse alla gestione di molteplici credenziali di accesso. Ogni persona di una certa organizzazione (scuola, università, ente di ricerca, …) potrà avere una identità unica (solo una username e una password) per accedere a tutte le risorse interne alla propria organizzazione e questa identità sarà valida anche per tutte le risorse esterne. Grazie all'identità federata l'insicurezza causata dall'avere un elevato numero di credenziali, viene ridotta o eliminata. La comodità dell'autenticazione con l'identità unica (federata) è apprezzata e questa identità diventa preziosa per l'utente che è portato automaticamente a conservarla con cura poiché è la chiave di accesso alle proprie risorse personali come la posta elettronica.

Il nucleo fondamentale di questo nuovo paradigma si attua tecnicamente rendendo l'organizzazione di appartenenza dell'utente l'unico gestore della sua identità. Le identità digitali non saranno più replicate sui servizi. Il codice di accesso è gestito dall'organizzazione di appartenenza dell'utente, per questo può essere protetto in modo opportuno e l'identità digitale può essere modificata o rimossa quando l'utente non ha più diritto di accedere alle risorse. Aumenta la fiducia da parte dell'utente che i propri dati personali siano al sicuro e non vengano usati abusivamente.

Come funziona tecnicamente

La gestione federata dell'accesso alle risorse diventa possibile quando istituzioni e fornitori di servizi si accordano per fidarsi reciprocamente delle informazioni scambiate e stabiliscono regole e linee di condotta per gestire queste relazioni di fiducia. Questi accordi prendono il nome di Federazione. Da 10 anni ad oggi sono nate federazioni di identità nel settore dell'istruzione e della ricerca in oltre 60 paesi[1] in tutto il mondo

[1] REFEDS, The Voice of Research and Education Identity Federations, https://refeds.org/federations

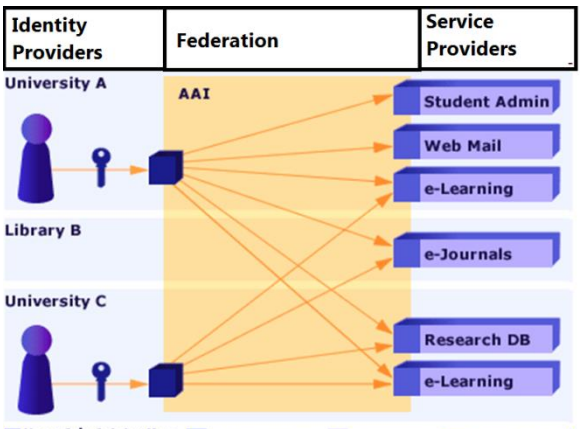


Figura 4

e nuove continuano a nascere. In Italia c'è IDEM (Identity Management per l'accesso federato)[2], promossa dal Consortium GARR[3]. Questo significa che tutti, dagli studenti, ai docenti, ai ricercatori, potranno utilizzare lo stesso sistema standard per la gestione degli accessi.

In una Federazione di identità i fornitori di servizi (Service Provider, SP) non gestiscono più gli utenti (Figura 4), non richiedono di compilare moduli di registrazione al servizio, non detengono più e non distribuiscono più codici di accesso e password. Tutte queste operazioni, che sono definibili come gestione delle identità (identity management) e gestione del processo di autenticazione vengono trasferite in carico alle organizzazioni di afferenza degli utenti (scuole, università, enti di ricerca, ecc…). Per effettuare le operazioni di identity management e di *autenticazione*, le istituzioni di afferenza degli utenti installano un sistema denominato Identity Provider (IdP). Ai SP rimane in carico il processo di *autorizzazione* degli utenti all'accesso. Dato che le asserzioni riguardanti gli utenti devono transitare dagli IdP verso i SP, la federazione si occupa di mettere in collegamento IdP e SP in modo fidato, con comunicazioni certificate e crittografate e provenienti da mittenti verificati. Si viene a creare un ecosistema dove ogni sistema partecipante (IdP o SP), avendo stipulato un unico accordo di fiducia con la federazione, può, grazie a questo unico accordo, fidarsi di tutti gli altri membri della federazione, presenti e futuri. La federazione si occupa anche di escludere dalla fiducia, e quindi dall'ecosistema, eventuali sistemi che non rispettino più gli accordi.

Esistono varie soluzioni tecnologiche per realizzare la gestione federata degli accessi. Esse implementano una serie di protocolli per lo scambio sicuro delle informazioni riguardanti le identità tra istituzioni e fornitori di servizi e adottano un approccio conforme allo standard SAML[4]. Shibboleth[5] è un esempio di questa tecnologia. All'interno della Federazione l'informazione su ciascun utente è detenuta soltanto dall'istituzione alla quale l'utente è affiliato e ciò significa che per ogni organizzazione esiste un singolo punto centrale di gestione delle identità (Figura 5).



Figura 6

Il caso d'uso di Moodle

Le istituzioni e i fornitori di servizi, a garanzia della privacy, preferibilmente non condividono informazioni personali sull'utente, ma si scambiamo informazioni riguardanti il diritto o meno di accedere alle risorse. Queste informazioni, dette attributi (Figura 6), possono semplicemente consistere nella dichiarazione che un utente è un insegnante o uno studente di una particolare università o scuola. Questo meccanismo si applica immediatamente a servizi di e-lernng basati su Moodle. L'utilizzo in Moodle della configurazione di autenticazione con Shibboleth[6] instrada l'utente a beneficiare dell'accesso facilitato mediante la sua identità istituzionale, permette di ridurre l'uso improprio di Moodle evitando la condivisione della password tra più utenti, infine l'utente capisce meglio il valore del tenere segreta la

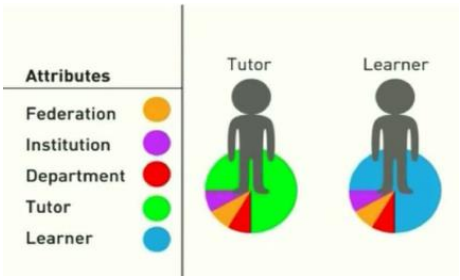


Figura 5

[2] Federazione IDEM, Identity Management per l'accesso federato, https://www.idem.garr.it/idem
[3] Consortium GARR, la Rete Italiana dell'Università e della Ricerca, http://www.garr.it/
[4] SAML, Security Assertion Markup Language, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
[5] Shibboleth is among the world's most widely deployed federated identity solutions, http://shibboleth.net/
[6] Configuring Moodle to use Shibboleth https://docs.moodle.org/29/en/Shibboleth

propria password. Il controllo fine dell'accesso a Moodle è facilitato e permette ad esempio creazione automatica dei gruppi di utenti che formano le classi[7]. Diventa immediato l'accesso al materiale didattico differenziato per classi. La gestione federata degli accessi riduce anche il carico di lavoro per la gestione delle credenziali che attualmente grava sul personale che amministra i sistemi di e-learning, lasciando loro tempo per concentrarsi sulla didattica o sui servizi aggiuntivi da offrire.

Il ruolo della federazione di identità

Una federazione di identità definisce un insieme di regole che ognuno dei membri, organizzazioni di utenti o fornitori di servizi, sottoscrive. Questo permette a tutti i membri di fidarsi vicendevolmente. Le scuole, le università, i centri di ricerca, le organizzazioni del settore pubblico e i partner commerciali possono tutti trarre vantaggio dell'approccio federato per l'accesso alle risorse. Il nuovo sistema permette agli utenti di autenticarsi presso la propria istituzione e ciò offre nuove opportunità di collaborazione e nuove possibilità di gestione degli accessi finora non disponibili, come ad esempio l'offerta di corsi condivisi tra più università o più scuole, oppure la condivisione e l'elaborazione on-line di materiale didattico da parte di più insegnanti che si trovano anche a distanze geografiche molto lontane tra loro.

Ad oggi alla Federazione IDEM in Italia aderiscono 116 SP e 72 IdP. Questi ultimi hanno attivato circa 4 milioni di identità digitali corrispondenti ad altrettanti utenti (studenti, docenti e personale degli enti membri). La Federazione IDEM è interfederata con le analoghe federazioni nel resto del mondo nella interfederazione eduGAIN che ad oggi nel mondo conta circa 1000 SP e altrettanti IdP. eduGAIN abilita gli utenti IDEM ad accedere con la propria password unica alle 1000 risorse federate[8] e similarmente conferisce agli SP di IDEM un potenziale bacino di decine di milioni utenti da tutto il mondo.

La Federazione IDEM, tramite il Servizio di assistenza denominato "IDEM GARR AAI" offre anche un ampio spettro di servizi: * un servizio di consulenza sia per SP che per IdP, per assistere le organizzazioni nei problemi di configurazione e risolvere gli errori di sistema relativi alle procedure di accesso sia in preproduzione che in produzione; * un servizio di IdP as a Service, nel caso che l'organizzazione non abbia le risorse per gestire l'IdP internamente; * un ambiente di federazione di test (sandbox); * servizio di pubblicazione di metadati e di profili di attributi che i membri possono usare; * un sistema di registrazione self-service per IdP e SP; * un servizio di discovery centralizzato ad uso degli SP; * un servizio di valutazione del *Level of Assurance* degli IdP; * guide di installazione e tutorial.

Conclusione/Abstract

I fornitori di servizi e di risorse on-line per la didattica e la ricerca, quali gli e-learning management system, i MOOCs, le piattaforme di social learning, le piattaforme collaborative, di condivisione, ecc…, oggi hanno l'opportunità di integrarsi nell'ecosistema delle federazioni di identità. Grazie alle federazioni di identità potranno offrire il loro servizio in una modalità estremamente più sicura, dove il furto di credenziali e la compromissione di sistemi non sarà più un problema a cui pensare. La gestione automatizzata degli utenti ed eventualmente dei gruppi e delle classi sarà più agevole e agli utenti non sarà più richiesto di compilare il noioso modulo di registrazione. Le scuole, come già fanno le università, possono completare i propri sistemi di identity management aggiungendo il componente identity provider mediante il quale possono attivare per tutti i propri utenti l'autenticazione unica verso tutte le risorse interne ed esterne all'organizzazione. La Federazione IDEM, promossa dal Consortium GARR, ha il ruolo di gestore dell'ecosistema di federazione e offre la tecnologia, le competenze e i servizi a valore aggiunto per agevolare e promuovere la diffusione della gestione dell'identità federata.

[7] Usare Grouper per gestire l'autorizzazione di Moodle, Biancini, Andrea; Mantovani, Maria Laura; Malavolti, Marco, Consortium GARR

[8] È possibile mostrare una live demo