Password da ricordare, dati da conservare… Dalla comunità GARR nasce la prima Federazione italiana di Infrastrutture di Autenticazione e Autorizzazione per semplificare l'accesso ai servizi

Carlo Volpe
Consortium GARR, The Italian Academic & Research Network

Semplice e veloce: è la "chiave" d'identità digitale

Dopo l'articolo di Franco Serio apparso nel numero scorso di BELTEL, *proponiamo ora, un altro interessante contributo in materia d'identità digitale, questa volta dagli amici della Comunità GARR – la rete telematica italiana dell'Università e della Ricerca scientifica e accademica italiana – il quale presenta un progetto che mira a semplificare e razionalizzare l'accesso ai servizi.*

Cosa può accomunare risorse molto differenti fra loro quali, ad esempio, la posta elettronica, una biblioteca, un programma di e-learning, un servizio di videoconferenza o una raccolta di pubblicazioni scientifiche?

Da oggi, grazie alla nascita della Federazione IDEM, può bastare una chiave. Ovvero un'unica chiave d'accesso, sempre identica per qualsiasi necessità. La sfida lanciata dalla comunità GARR è senz'altro ambiziosa e impegnativa, ma degna del sogno di semplificare la vita a ricercatori e docenti razionalizzando l'accesso ai servizi e riducendo la complessità dovuta all'utilizzo di molteplici credenziali. Finora infatti per fruire di qualsiasi servizio o contenuto on-line l'utente aveva bisogno di registrarsi e ricevere un codice di accesso. Tale procedura spesso veniva replicata più volte con conseguenti problemi sia per l'utente che per l'organizzazione. Molte password da ricordare, dati da conservare in siti differenti e duplicazione delle operazioni burocratiche: difficoltà che presentavano spesso ricadute anche in termini di tutela della riservatezza e protezione dei dati, nonché un maggior carico di lavoro e perdite di tempo per il personale amministrativo.

A disposizione della comunità accademica e scientifica italiana, ora invece, è presente un servizio nuovo, una vera e propria federazione di Infrastrutture di Autenticazione e Autorizzazione (AAI). Una AAI permette di separare le due fasi essenziali di ogni procedura di controllo dell'accesso: quella dell'autenticazione, in cui si verifica l'identità dell'utente e quella dell'autorizzazione in cui si accerta che egli abbia effettivamente diritto all'utilizzo della risorsa. Ogni organizzazione stabilisce un sistema di autenticazione per verificare l'identità dei propri utenti e fornisce loro un'unica credenziale valida per accedere a qualsiasi servizio. L'organizzazione quindi trasferisce alla risorsa gli attributi, cioè alcune caratteristiche dell'utente opportunamente rese anonime, che la mettono in grado di decidere se concedere o meno l'accesso a chi ne ha fatto richiesta.

Una federazione collega differenti organizzazioni che, aderendo ad una serie di accordi e di regole condivise, si impegnano a consentire lo scambio di attributi degli utenti in maniera sicura, tutelando la privacy e il diritto alla riservatezza. Grazie all'approccio federato, i vari soggetti in campo sono coinvolti congiuntamente per garantire un ambiente di fiducia. In questo modo tutti possono trarne dei vantaggi: dalla parte degli utenti c'è una riduzione delle password da

ricordare e la semplificazione dell'accesso alle risorse; per gli enti membri, una riduzione dei costi nella gestione delle utenze e nella realizzazione di nuovi servizi; per i fornitori di risorse, una riduzione del carico amministrativo e la possibilità di estendere il proprio bacino d'utenza.

Dal progetto al servizio

La realizzazione della prima federazione italiana di AAI è il frutto di un lungo lavoro, avviato nel 2007 con il progetto pilota IDEM (IDEntity Management) coordinato da GARR e che ha coinvolto una trentina di istituzioni e fornitori di servizi per un totale di circa 700.000 utenti. La fase di sperimentazione è stata decisiva per testare la fattibilità, l'operatività, l'utilità e l'usabilità di una federazione AAI e per acquisire esperienza utile a predisporre l'infrastruttura tecnico-amministrativa necessaria per lo sviluppo del servizio vero e proprio.

Concluso il progetto pilota, la Federazione è pronta ora a ricevere le prime adesioni, che possono essere di due tipi: come "membri" o come "partner".

Entrare nella Federazione

Concluso il progetto pilota, la Federazione è pronta ora a ricevere le prime adesioni, che possono essere di due tipi: come "membri" o come "partner". Entrano come membri le organizzazioni che fanno parte della comunità GARR, mentre come partner le altre organizzazioni che hanno interesse a condividere i propri servizi. Si tratta, ad esempio, di fornitori di informazioni e di contenuti anche multimediali (editori scientifici, archivi digitali, ecc.), fornitori di servizi on-line (download di software, musica, acquisto di biglietti, accesso a dati scientifici di laboratori non statali, ecc.), fornitori di servizi per i cittadini (servizi anagrafici, servizi sanitari, pagamenti, ecc.). Nel corso del progetto pilota sono stati già stipulati diversi accordi di questo genere come quelli con editori scientifici quali Elsevier, Springer e Thomson Reuters.

Per partecipare alla Federazione è necessario che ogni organizzazione registri almeno un proprio servizio che può essere un Identity Provider (IdP), cioè un servizio di gestione e verifica delle identità, oppure un Service Provider (SP), ovvero una risorsa accessibile in rete. I membri della comunità GARR partecipano alla Federazione prevalentemente registrando un IdP ma possono anche registrare risorse e servizi, come ad esempio hanno già fatto l'Università degli Studi di Modena e Reggio Emilia con una piattaforma di e-learning, l'Università degli Studi di Torino con un blog e il CASPUR con un wiki. Per registrare un IdP è necessario che l'organizzazione predisponga al proprio interno un sistema di Identity & Access Management che permetta la registrazione degli utenti in modalità controllata e faccia in modo che gli attributi dell'utente siano resi disponibili e utilizzati dagli altri partecipanti nel rispetto della normativa vigente sulla privacy e delle regole della Federazione. Per registrare una risorsa, invece, il fornitore di servizi e contenuti deve garantire il trattamento dei dati ricevuti secondo liceità e correttezza e descrivere le modalità e i requisiti per l'accesso.

L'adesione alla Federazione comporta inoltre il rispetto di alcune specifiche tecniche: l'infrastruttura di IDEM si basa infatti su Shibboleth ed è pertanto necessario dotarsi di questo software o di un'altro equivalente che sia compatibile con lo standard SAML2.0. Nell'ambito della Federazione IDEM, GARR agisce da coordinatore centrale, sottoscrive i Contratti d'Adesione e mette a disposizione un servizio tecnico-amministrativo di supporto. Tramite questo servizio denominato IDEM GARR AAI sono forniti ai partecipanti il catalogo e i metadati dei servizi (IdP e risorse) presenti nella Federazione, il know-how per l'implementazione dei servizi attraverso attività di help-desk, formazione e aggiornamento, il discovery service (WAYF) e un sito web dove reperire informazioni e documentazione. Viene svolta inoltre un'attività di monitoraggio e auditing.

L'avvio del servizio è un segnale importante che lascia intravedere anche la possibilità di estendere la collaborazione con altre federazioni per integrare i diversi sistemi e raggiungere un numero di utenti e di servizi sempre più ampio. In questa direzione sono significative alcune esperienze della Pubblica Amministrazione come quella avviata in Emilia-Romagna con il progetto FedERa (Federazione degli enti dell'Emilia-Romagna per l'autenticazione) o quella del progetto ICAR (Interoperabilità e Cooperazione Applicativa in rete tra le Regioni) che coinvolge sedici regioni e una Provincia Autonoma.

Questo articolo è tratto dalla rivista semestrale GARR News, che ringraziamo. Maggiori informazioni sul regolamento e sulle procedure d'adesione alla Federazione IDEM sono disponibili sul sito: www.garr.idem.it.