Un(')utente/una password per l'accesso alle risorse e ai servizi online

Bonaria Biancu – Università Milano Bicocca

L'intervento poggia su due concetti: (le nuove forme di) identità digitale e accesso ai contenuti.

In questo contesto, con "identità digitale" si intende "identità in senso *tecnico*", cioè quell'insieme di informazioni relative a un appartenente a una organizzazione, che si coagulano intorno a un *Identifier* (solitamente lo username assegnato ai singoli appartenenti), un *Authentifier* (solitamente la password) e gli *attributi* (le caratteristiche attraverso le quali il singolo viene riconosciuto dall'organizzazione: qualifica, ruolo, rapporto di lavoro, ufficio, eventuali ulteriori gruppi interni etc.)[1]. Username e password compongono le credenziali che vengono associate, all'interno di una organizzazione, a tutti coloro che ne fanno parte. Gli attributi determinano le risorse e i servizi cui il singolo può accedere, ed eventualmente anche le modalità di accesso (es.: con certi diritti, per una durata specifica etc.).

Le credenziali e gli specifici attributi fanno parte del framework di autenticazione-autorizzazione che viene attivato ogni qual volta un utente desideri accedere a una specifica risorsa non presente in accesso aperto sul web (es.: le riviste elettroniche a pagamento) oppure debba utilizzare un applicativo (es.: il modulo di rinnovo prestiti di un OPAC) o ancora voglia usufruire dei servizi di una piattaforma (es.: video-conferenza, document delivery etc.).

Le credenziali e gli attributi sono perciò legati a un certo dominio applicativo e circoscrivono l'ambito di sicurezza entro il quale l'organizzazione autorizza l'utente ad agire. Inoltre l'organizzazione si fa garante verso l'utente di osservare i requisiti previsti dalla legge per quanto riguarda i suoi dati personali e la sua privacy.

---

1 Per semplicità ci limitiamo qui a discutere il caso più comune nelle nostre organizzazioni: l'identificazione dell'appartenente a una organizzazione mediante credenziali istituzionali. Vi sono però altre modalità di autenticazione/autorizzazione: dai certificati digitali ai token alle impronte biometriche, modalità che spesso vengono usate in combinazione con le credenziali per consentire di usufruire di ulteriori servizi all'interno dell'organizzazione (accesso a luoghi fisici come i laboratori o i parcheggi o alle singole postazioni di lavoro, svolgimento di particolari operazioni come la firma dei verbali di esame digitali e così via)..

Le modalità di accesso ai contenuti e ai servizi di una biblioteca fisica e digitale sono svariate, e spesso funzione della tipologie di risorse e servizi. Dall'ingresso di un utente nella biblioteca fisica, al collegamento a Internet (mediante wi-fi o accesso ai terminali), all'accesso a banche dati bibliografiche su CD-ROM, al download del full-text di riviste elettroniche o e-book, all'utilizzo di strumenti per la creazione di bibliografie, OPAC, Learning Management System e così via, spesso l'utente si trova a fronteggiare una varietà elevata di modalità di autenticazione, e perciò di memorizzazione/gestione credenziali.

Le modalità prevalenti per usufruire di una risorsa o di un servizio sono ad oggi: l'autenticazione mediante credenziali e l'accesso via IP. Entrambe però non sono esenti da difetti e problematiche tecniche e gestionali.

Nel caso, frequente, di utilizzo di credenziali 'locali' a singole risorse o servizi, l'utente deve memorizzare username e password diverse, ad esempio, per il rinnovo di un prestito, la creazione di ricerche personalizzate sul discovery tool; l'accesso a una banca dati; per collegarsi a Internet mediante wi-fi dovrà utilizzare un certificato; per entrare fisicamente in biblioteca dovrà esibire un badge. Se poi vuole consultare la posta istituzionale deve utilizzare le credenziali istituzionali, ma le stesse non le/gli servono se deve svolgere un compito nel LMS del corso di laurea che sta seguendo (credenziali rilasciate dal LMS). Nel caso l'utente si trovi poi fuori dalla rete di Ateneo, le cose si complicano: potrà usare comunque alcune risorse o applicativi (credenziali 'locali'); per gli altri invece, cioè quelli il cui accesso è regolato in base all'indirizzo IP di provenienza, deve utilizzare (se la sua organizzazione ne dispone) un proxy o una VPN: in pratica, cioè, deve simulare di essere in rete su un IP della biblioteca. Per utilizzare proxy e VPN, però, occorre seguire alcune procedure di configurazione, il che può non essere immediato per tutti gli utenti (curva di apprendimento) e comunque richiede ancora una volta l'uso delle credenziali istituzionali per poter materialmente entrare nella rete della biblioteca.

Se dal punto di vista dell'utente le cose sono complicate, anche le organizzazioni (in questo caso le biblioteche e le istituzioni di cui fanno parte) e i fornitori/editori devono farsi carico di gestire la mole delle informazioni riguardanti le singole organizzazioni, i loro utenti (con profili e diritti associati), le policy diverse relative alla protezione dei dati personali. Inoltre, dal punto di vista delle organizzazioni, nel caso di attivazione di proxy per l'accesso dall'esterno, non tutti i browser sono compatibili con i servizi proxy, e, oltre a gestire lunghi elenchi di siti web autorizzati all'accesso mediante proxy, la biblioteca si deve anche fare carico di attivare un help desk dedicato.

La soluzione a queste problematiche che si intende prospettare, è il Single Sign On (SSO): si tratta di una modalità di garantire all'utente l'utilizzo delle stesse credenziali anche nell'accesso a risorse/servizi forniti da provider diversi. L'utente viene identificato e autorizzato dalle credenziali istituzionali (cioè

quelle rilasciate dall'organizzazione di appartenenza) – e non solo per applicativi o risorse dell'organizzazione (OPAC, webmail, LMS etc.) bensì per applicativi o risorse di altre istituzioni, di editori, di aggregatori e così via. Username e password[2] sono le uniche credenziali che l'utente deve memorizzare; sono gestite in sicurezza dall'istituzione di appartenenza; garantiscono l'accesso alle risorse pur senza essere condivise con terze parti. La stessa istituzione, inoltre, all'atto di confermare al provider che l'utente che sta cercando di accedere a una risorsa è legittimato a farlo, può riservarsi di rilasciare alcune informazioni che possono essere utili sia al fornitore (affiliazione dell'utente, appartenenza a un determinato gruppo etc.) sia all'utente medesimo (memorizzazione delle scelte effettuate in precedenza dall'utente su quella risorsa etc.).

Come avviene la comunicazione tra i provider e le organizzazioni per ottenere conferma della legittimità di un utente ad accedere a una risorsa, e come è possibile per le istituzioni rilasciare la conferma senza condividere al contempo le credenziali? Grazie al SSO federato: autenticazione e autorizzazione avvengono una sola volta e soltanto a opera dell'ente di appartenenza dell'utente, ma, poiché sia l'organizzazione sia il provider fanno parte di una stessa federazione, il provider sa riconoscere il tipo di utente che cerca di accedere a una risorsa, come appartenente a una certa organizzazione; prima di consentire l'accesso, perciò, re-invia l'utente ad autenticarsi verso l'organizzazione di appartenenza; se tutto va a buon fine, l'organizzazione di appartenenza conferma che l'utente è autorizzato ad accedere alla risorsa ed aggiunge ulteriori informazioni che consentono di identificare in maniera pseudonima l'utente medesimo, al fine di abilitare i benefici visti sopra per entrambi i partner della comunicazione. L'efficacia e l'efficienza della gestione delle credenziali sono garantite, sia per l'utente sia per l'organizzazione sia per i fornitori; allo stesso modo l'utente sa che la organizzazione cui appartiene rilascerà solo le informazioni necessarie e in maniera protetta.

Esistono a livello nazionale e internazionale diverse tipologie di federazioni di identità: in Italia la più nota è IDEM[3], dedicata al mondo delle università e degli enti di ricerca. IDEM conta diverse decine di membri (atenei ed enti), partner (fornitori, editori etc.) e risorse condivise. A livello tecnologico, IDEM adotta il

2 Anche in questo caso ci riferiamo per semplicità alle credenziali di tipo username/password; l'utente potrebbe essere in realtà riconosciuto e autorizzato dalla propria istituzione anche mediante altri dispostivi, ad esempio con un certificato digitale.

3 https://www.idem.garr.it/index.php.

framework Shibboleth ma è in generale compliant con ogni applicativo basato su SAML, il 'dialetto' XML utilizzato dalle organizzazioni e dagli enti delle federazioni per 'riconoscersi', comunicare e scambiarsi informazioni sugli utenti.

L'organizzazione all'interno di IDEM è bipartita in IdP (Identity Provider), cioè le organizzazioni che forniscono asserzioni sui loro utenti ai provider che ne fanno richiesta, e SP (Service Provider), cioè editori, aggregatori, produttori di applicativi etc. ai quali l'utente chiede l'accesso. Quando un'utente di una organizzazione che aderisce a IDEM desidera accedere a una risorsa il cui fornitore appartiene ugualmente alla Federazione, è finalmente affrancata dalle problematiche relative a indirizzi IP, recupero credenziali, proxy, sistemi di autenticazione o postazioni dedicate: deve semplicemente scegliere, sulla risorsa, la modalità di autenticazione federata (le etichette possono essere diverse: da "SSO" a "Shibboleth" a "Institutional Login"), quindi selezionare la federazione di appartenenza (nel nostro caso: IDEM): verrà rediretta sulla pagina di autenticazione della propria organizzazione, per l'inserimento di username e password. Se la procedura va a buon fine, l'organizzazione restituisce al fornitore la conferma che l'utente è autorizzata ad accedere insieme a un identificativo permanente, oltre ad asserzioni sull'utente medesima (ad esempio: l'utente è di tipo 'docente'; è affiliata a un certo dipartimento etc.). Il fatto che l'organizzazione e il fornitore identifichino l'utente mediante un ID univoco e persistente, consente, tra l'altro, di ottenere anche statistiche mirate e puntuali sull'utilizzo delle risorse (ciò che la semplice identificazione mediante indirizzo IP non può ovviamente garantire).

Come dimostra un recente studio del NISO[4] (divenuto nell'ottobre 2011 una *recommended practice*), all'interno di uno scenario di comunicazioni sempre più interconnesso, che vede moltiplicarsi i punti di accesso a risorse e servizi e i device utilizzati dagli utenti, e che è sempre meno legato alla localizzazione fisica (IP) dell'organizzazione e sempre più ai diritti che l'organizzazione garantisce ai suoi utenti ovunque si trovino, l'accesso mediante credenziali duplicate e/o mediante indirizzo IP si rivela poco efficiente. È necessario evolvere verso scenari nei quali l'utente affiliato a una organizzazione possa portare con sé, nella Rete, la propria identità e gli attributi a essa legati. Alcuni segnali denotano il radicamento progressivo delle federazioni di identità nel mondo delle biblioteche digitali: i contratti nazionali CARE, stipulati tra gli atenei italiani e alcuni grandi editori, tra le varie clausole contengono anche la richiesta di adeguamento alle tecnologie dell'autenticazione federata per agevolare l'accesso libero e ubiquo degli utenti degli atenei a e-journals e e-book; i consorzi CILEA e CASPUR hanno portato le loro digital library all'interno

4 http://www.niso.org/workrooms/sso.

della federazione IDEM; alcuni tra i principali vendor di software per le biblioteche, hanno reso i loro applicativi compatibili con le tecnologie del SSO.

Naturalmente i vantaggi dell'autenticazione federata saranno massimi quando tutte le risorse entreranno a far parte delle federazioni e garantiranno agli utenti l'utilizzo delle sole credenziali istituzionali per poter accedere a- e usufruire di- risorse e servizi. Fino ad allora, è necessario lavorare per estendere la consapevolezza dell'utilità (e per certi versi dell'ineludibilità) dell'autenticazione federata, avvalendosi di strumenti, come alcuni tipi di proxy[5], che offrono all'utente una esperienza di accesso e fruizione dei contenuti *seamless* e intuitiva, sostenendo dietro le quinte sia l'autenticazione mediante credenziali (per quelle risorse compliant) sia quella mediante indirizzo IP di provenienza.

L'accesso mediante IP è stato una grande conquista, ma per evolvere verso i nuovi scenari disegnati dall'agenda digitale e dalla e-Science (condivisione e utilizzo integrato di infrastrutture, risorse di calcolo, dati, informazioni) è auspicabile che le biblioteche recuperino lo slancio collaborativo che ha sempre caratterizzato la loro storia, per compiere un ulteriore passo avanti sulla strada di quella rivoluzione copernicana che sembra prospettarsi: saranno sempre più le risorse e i servizi a ruotare intorno all'utente, e sempre meno questi a doversi adattare alle prime. Le biblioteche e i fornitori sono chiamati a garantire e realizzare insieme questa transizione.

5 Si veda per esempio l'EZProxy http://www.oclc.org/ca/en/ezproxy/default.htm.