Questo estratto è un materiale di supporto realizzato a beneficio dei partecipanti all'IDEM Biblioday 2012 (Milano, Palazzo delle Stelline, 16 Marzo 2012) tratto dal documento: "ESPReSSO: Establishing Suggested Practices Regarding Single Sign-On", pubblicato da NISO - National Information Standards Organization, Baltimore, Maryland, U.S.A. (rif. pubblicazione NISO RP-11-2011 – ESPReSSO).
Il documento è pubblicato integralmente su: http://www.niso.org/publications/rp/RP-11-2011_ESPReSSO.pdf

ESPReSSO: stabilire buone pratiche per il Single Sign-On

Negli ultimi anni, molte istituzioni si sono mosse per trarre vantaggio dai molti benefici del Single Sign-on, tra cui l'accesso a *learning management system* (es. Blackboard, Sakai), strumenti di Ricerca (es. RefWorks, TurnItIn) e, ovviamente, risorse basate sulla sottoscrizione di un abbonamento (es: *e-journal*, *e-book*, database). Far funzionare meglio e in modo più intelligente il Single Sign-On (SSO) permetterà agli utenti di avere un maggiore successo nell'accedere ai contenuti e servizi ai quali hanno diritto. Negli ultimi anni, molti dei più grandi *service provider* (SPs) hanno implementato tecnologie di SSO. D'altra parte, va detto che molti di quanti ospitano contenuti non lo hanno fatto. Gli utenti delle biblioteche si trovano quindi ad operare in un ambiente che include un insieme di tecnologie di autenticazione, tra cui quelle che utilizzano l'IP dell'utente sono le più diffuse. Una soluzione efficiente al problema deve quindi indirizzarsi a questo ambiente ibrido e, come minimo, prendere in considerazione la necessità di *proxy* di autenticazione IP, nonché il modo in cui questi interagiscono con le tecnologie di tipo SSO.
Il documento di buone pratiche di ESPReSSO raccomanda soluzioni pratiche e delinea una strategia per migliorare il successo delle tecnologie di autenticazione SSO nel fornire un'esperienza di utilizzo quanto più possibile trasparente. Inoltre, il documento mira a promuovere l'adozione da parte di università e fornitori di servizi di una famiglia di soluzioni in grado di rendere il miglioramento dell'accesso una realtà. Questa iniziativa non ha inventato alcuna nuova tecnologia o protocollo, piuttosto ha sviluppato un insieme di buone pratiche relative all'utilizzo di tecnologie esistenti.
Il gruppo di lavoro di ESPReSSO si è innanzi tutto preoccupato della situazione in cui un'organizzazione (università, biblioteca pubblica, aziende, etc) acquisisce una licenza per accedere a contenuti specifici erogati attraverso il web, e in cui l'utente è un membro dell'organizzazione autorizzato ad accedere quel contenuto. Il gruppo di lavoro non ha preso in considerazione la situazione in cui un individuo, singolarmente o come parte di un gruppo, ottenga una licenza individuale per uso personale e quindi utilizzi un *account* personale per autenticarsi con il service provider. I *service provider* riferiscono infatti che al momento gli utenti non richiedono questo tipo di funzionalità. Inoltre, supportare questo approccio richiede da parte gli editori tanto lavoro nella gestione delle credenziali degli utenti quanto da parte dell'organizzazione licenziataria. Il processo che gli editori utilizzano per vendere articoli singoli non rientra nell'ambito di questo documento.
Le buone pratiche relative all'esperienza di utilizzo da dispositivo mobile stanno evolvendo molto rapidamente, di conseguenza questo documento si astiene dal formulare raccomandazioni specifiche per questo tipo di utilizzo. In ogni caso, i flussi descritti nel documento possono essere applicati anche a dispositivi mobili. Un ultimo aspetto da tenere in dovuta considerazione è, come per tutti i sistemi basati su web, quello dell'accessibilità. Il documento presenta, a titolo di esempio, alcune implementazioni, senza però raccomandarne una specifica. Ogni implementazione dovrebbe rispondere alle *Web Content Accessibility Guidelines* (WCAG).

Termini e definizioni

***service provider* (SP) -** un sito web che offra servizi e contenuti agli utenti. Spesso una parte del sito è aperta alla navigazione pubblica, mentre l'accesso ad un'altra parte è controllato e richiede la prova che l'utente sia autorizzato ad accedere nell'ambito di un contratto esistente. Molti editori di contenuti offrono contenuti su licenza in Internet.

***identity provider (IdP)* -** l'organizzazione di appartenenza di un utente. L'utente tipicamente ha una relazione forte con questa organizzazione, ed essa può fare asserzioni aggiornate e accurate sull'utente.

***identity discovery service* -** una pagina web sulla quale i *service provider* reindirizzano l'utente per l'autenticazione, dopo che questo ha selezionato la sua istituzione d'appartenenza. Questa pagina veniva in precedenza chiamata servizio WAYF ("*Where Are You From*").

***deep link* -** una URL che punta ad una specifica risorsa (es. un articolo) sul sito di un *service provider*.

login (o autenticazione) federata - un approccio all'autenticazione in cui il sito di un *service provider* reindirizza l'utente alla propria organizzazione di appartenenza per l'autenticazione. Dopo che l'autenticazione è andata a buon fine, l'utente è reindirizzato nuovamente al *service provider*, accompagnato da asserzioni di attributi che descrivono i suoi diritti presso il *service provider*. Nel documento, il termine include il processo di autorizzazione realizzato sul sito del SP.

federated search (metasearch; web-scale discovery search) - un portale che permette ad un utente di inserire termini di ricerca e poi li utilizza per effettuare ricerche attraverso un gran numero di fonti potenziali, permettendo così di rintracciare tutti i contenuti con licenza rilevanti, senza necessariamente conoscerne a priori l'ubicazione.

IP-based authentication - un metodo di autenticazione in cui un SP e una organizzazione licenziataria concordano che ogni richiesta che venga da un certo insieme di indirizzi IP associati con l'organizzazione licenziataria ha diritto ad accedere le risorse oggetto della licenza.

Just-in-Time (JIT) authentication - un processo sul sito di un SP che dà inizio alla procedura di login quando un utente anonimo cerca di accedere ad un contenuto ad accesso controllato. Ad esempio, una JIT verrà innescata se un utente anonimo cerca di accedere ad un *deep link*.

organizzazione licenziataria - l'istituzione che ha sottoscritto un contratto con un service provider a beneficio di utenti che sono in qualche modo affiliati a quella istituzione. L'organizzazione licenziataria diventa quindi l'*identity provider* per questi utenti. In questo documento si usa talvolta la parola "campus" per riferirsi all'organizzazione licenziataria.

link resolver - Un servizio gestito dalla organizzazione licenziataria, che accetta una sintassi OpenURL (es. da un sito che contenga degli abstract) e la mappa su un sito in cui l'organizzazione licenziataria ha accesso ad una copia su licenza dell'articolo completo.

personally identifiable information (PII) - informazione che rende possibile identificare un particolare individuo. Un nome di persona è considerato PII (benché esso possa non essere sufficiente per identificare in modo esclusivo una singola persona). Il documento fa riferimento a situazioni in cui un *identity provider* può fornire ad un service provider attributi che contengono questo tipo di informazione.

proxy server - un sistema informatico che agisce da intermediario tra un utente che fa una richiesta ed il servizio richiesto. Le organizzazioni licenziatarie mantengono dei *proxy servers* per fornire accesso a risorse su licenza ai loro utenti, quando questi non siano direttamente connessi alla rete dell'organizzazione (es da casa o in mobilità). Gli utenti si autenticano sul *proxy*, che a sua volta è connesso alla rete dell'organizzazione, e il proxy permette di accedere alle risorse per suo tramite.

security assertion markup language (SAML) - un approccio standardizzato all'autenticazione single sign-on (SSO) sul web. Esistono molte soluzioni SAML interoperabili tra loro, sia *open source* che proprietarie.

virtual private network (VPN) - un metodo sicuro per interconnettersi alla rete protetta di un'organizzazione da remoto, attraverso un server che autentica l'utente remoto utilizzando le credenziali fornite dall'organizzazione. L'utente autenticato sulla VPN appare al *service provider* come proveniente da un IP dell'organizzazione licenziataria, anche se l'utente si trova fisicamente in un luogo diverso.

URL WAYFless - una URL creata dall'organizzazione licenziataria contenente informazione su di essa, che punta a un *service provider*. Selezionare una URL WAYFless permette ad un utente di bypassare il processo di *Identity Discovery*.

autenticazione web single-sign on (SSO) - un *framework* per autenticare gli utenti attraverso famiglie di servizi. L'utente si autentica una sola volta e le successive richieste di autenticazione vengono gestite in modo trasparente dal servizio, senza richiedere altre azioni da parte dell'utente.

Raccomandazioni

La seguente sezione contiene un sommario delle raccomandazioni del gruppo di lavoro nei riguardi di service provider e organizzazioni licenziatarie, al fine di avere delle implementazioni di successo e una positiva esperienza di utilizzo. Il loro principio informatore è la coerenza, intesa in due sensi:

1) Coerenza tra i servizi: studi hanno dimostrato che la mancanza di coerenza tra diversi SP è la prima causa di confusione per gli utenti. Le persone sono in grado di adattarsi a *workflow* complicati, purché essi siano familiari, mentre *workflow* semplici costituiscono una barriera se sono nuovi. Può essere difficile convincere i proprietari delle applicazioni, spesso convinti di avere un bisogno particolare di differenziarsi, che gli utenti hanno bisogno di questo. L'esperienza invece suggerisce che la strategia del "differenziarsi" ha in questo caso dei costi in termini di training degli utenti e rifiuto degli stessi ad usare il servizio, e che la federazione diventa il capro espiatorio.
2) Coerenza della "storia" attraverso il processo. L'esperienza suggerisce che l'utente reagisce meglio quando la transizione tra i vari passi del processo mantiene un grado di coerenza rispetto al linguaggio e alla presentazione utilizzati. Gli utenti vogliono che il contesto in cui si svolge l'azione (loggarsi nel SP attraverso l'IdP) sia chiaro ad ogni passo. Se l'interfaccia cambia in modo stridente e/o manca di un riferimento visivo e testuale all'obiettivo o attività generale, essi si trovano disorientati più facilmente. Un gran numero di nuove funzionalità del software e iniziative di federazione (es. User Interface Elements) fanno riferimento a questo bisogno.

Pagina di apertura dell'SP

- La pagina di apertura del SP dovrebbe mostrare all'utente anonimo un link di login posizionato e etichettato nel modo preferito/raccomandato, che dovrebbe rimandare ad una pagina di *identity discovery*, annidata nel sito dell'SP.
- La pagina di apertura del SP dovrebbe anche supportare il controllo degli accessi basato su IP.

Pagina di identity discovery dell'SP

- Il SP dovrebbe fornire, all'interno del suo sito, una pagina di *identity discovery* che offra agli utenti anonimi che necessitino dell'autenticazione per accedere ad un contenuto protetto un processo per identificare la loro organizzazione di appartenenza (cioè l'organizzazione licenziataria del contenuto). Questa pagina dovrebbe:
  - essere caratterizzata graficamente come parte del SP;
  - in quanto veicolo di transizione, permettere uno o più meccanismi di autenticazione oltre a quello federato;
  - offrire un *search box* con suggerimenti automatici per trovare istituzioni per nome o nickname;
  - ricordare, attraverso l'uso di *cookies*, l'istituzione selezionata dell'utente in visite precedenti, offrendo un collegamento diretto o automatico alla pagina di login dell'organizzazione (il logo dell'istituzione, ottenuto attraverso i metadati, può essere utile a tal fine). La pagina di login dell'istituzione è controllata dall'organizzazione selezionata, non dal SP;
  - scelte preferite o ricordate devono essere sottolineate, ma non scelte automaticamente (cioè non è raccomandato l'uso di comportamenti automatizzati quali "usa questa scelta la prossima volta");
  - NON deve richiedere user id e password, perché l'utente potrebbe non realizzare che non si trova ancora sul sito della propria organizzazione. Gli utenti che sanno che dovranno utilizzare credenziali fornite dal *vendor* per accedere dovranno selezionare questa preferenza cliccando un link che indirizza al form di autenticazione del *vendor*[1]. Il design del flusso dell'interfaccia del processo di *discovery* dovrebbe ridurre la possibilità di questa confusione offrendo un form del *vendor* solo a quegli utenti che lo richiedono espressamente;
  - Offrire sempre le opzioni "aiuto" e "indietro".
- I SP potrebbero prendere in considerazione ulteriori caratteristiche del *discovery*, quali:
  - geo-localizzazione dell'IP dell'utente, per suggerire istituzioni prossime;

[1] È stato dimostrato che gli utenti non riescono sempre a distinguere chi sta richiedendo loro le credenziali quando gli viene presentato un form di login. L'utente quindi potrebbe per errore inserire il proprio nome istituzionale e la password associata nel form di login del vendor. Inoltre, presentare un form di login del vendor a un utente che non se lo aspetta potrebbe essere interpretato come un tentativo di "*phishing*" da alcune istitizioni.

- possibilità di ricerca delle istituzioni per città o codice di avviamento postale;
- link a metodi di autenticazione *legacy*, come form forniti dal *vendor* o Athens;
- possibilità di cambiare l'istituzione preferita dall'utente (se ricordata dal *cookie* del browser).

Pagine protette del SP

- Quando riceve richieste di pagine protette, il SP dovrebbe continuare ad utilizzare in prima battuta tecniche di login automatiche, prima di determinare se l'autenticazione SSO è richiesta per l'utente.
- Quando le richieste di pagine protette siano inoltrate alla pagina di *identity discovery*, il SP dovrebbe reindirizzare l'utente alla pagina originariamente richiesta dopo una autenticazione riuscita.

Pagina di login dell'IdP/Organizzazione licenziataria

- Questa pagina dovrebbe utilizzare il *branding* istituzionale dell'organizzazione, così da suggerire all'utente quali credenziali gli sono richieste.
- Questa pagina dovrebbe inoltre riportare il *branding* del SP per offrire all'utente un feedback sul fatto che la pagina di login dell'IdP è una parte normale del processo di autenticazione.

Pagina di catalogo dell'IdP/Organizzazione licenziataria

- Se l'organizzazione mantiene una pagina contenente un catalogo dei *database* e delle riviste sottoscritte, insieme ai link a queste risorse il menu dovrebbe supportare gli utenti anche nel caso non siano sulla rete interna dell'istituzione (e quindi non possano utilizzare l'autenticazione basata sull'indirizzo IP);
- L'utilizzo di URL WAYFless può semplificare il flusso di informazioni per gli utenti associati all'istituzione che fornisce il menu.

Proxy server in un ambiente ibrido

- Insieme al *proxy server* dovrebbe essere utilizzato un Access Mode Switch.
- È meglio fornire la URL del SP nella stringa di richiesta inviata al *proxy* (che sarà stato configurato per riconoscere i IdP rilevanti) piuttosto che fornire l'informazione appropriata dell'IdP all'interno della stringa inviata al SP.

Riscrivere le open URL

- È bene fare in modo che il *link resolver* sia configurato per produrre URL WAYFless.
- Le URL WAYFless possono semplificare il flusso per utenti associati all'istituzione che fornisce il menu.

Uso appropriato del branding del SP e dell'IdP

- Il SP dovrebbe utilizzare il proprio *branding* (logo, colori, grafica) nella pagina dell'*identity discovery* e nella pagina di login dell'istituzione.
- L'organizzazione licenziataria dovrebbe inserire il proprio *branding* nella pagina di login dell'organizzazione e, nel caso in cui l'utente abbia preselezionato un IdP, in quella di *identity discovery* di un SP.

Funzionalità aggiuntive

- Il SP dovrebbe supportare accessi con pseudonimo, ad esempio attraverso l'uso del tag "eduPersonTargetedID"
- Agli utenti dovrebbe essere presentata una richiesta di "consenso dell'utente al rilascio di attributi" prima che l'istituzione possa rilasciare informazione atta ad identificare una persona (PII) al SP.

Gestione degli errori

- La gestione dell'errore dovrebbe essere integrata all'interno del *look & feel* del sito.
- Il SP dovrebbe rendere chiaro quando un problema ha luogo.
- Gli errori che derivano da azioni dell'utente che possono essere corrette o evitate devono essere presentati in modo che diano luogo ad auto-correzione.
- Dovrebbero essere forniti procedure per riportare l'errore e informazioni di contatto e che portino ad una risoluzione.