Modifiche alle regole di composizione della pagina di login degli IdP

F. Lombardi, C. Marotta

vers. 1.0 - Ottobre 2010

Premessa

Durante la riunione del CTS dello scorso 27 Settembre, è emerso un problema legato alla scarsa aderenza ai requisiti richiesti da IDEM di pagine web di login relative ad alcuni IdP. Il CTS ha assegnato il compito di risolvere la questione agli scriventi [1].
Scendendo nel caso specifico, il problema è scaturito con la verifica della pagina di login dell'IdP di Milano Bicocca che risulta essere priva di qualsiasi riferimento alla Federazione IDEM [2]. Il problema si riassume citando il gestore dell'IdP interessto:

> *"Il CAS è utilizzato anche da una varietà di altri servizi Web interni che NON sono federati, perciò inserire informazioni esclusivamente di pertinenza di IDEM sulla stessa finestra di login che viene acceduta anche percorrendo "strade" completamente diverse (e distinte da quelle della federazione) potrebbe essere ambiguo e causare confusione."*

Analisi del problema

Le linee guida per la composizione della pagina di login sono contenute nel Documento Specifiche Tecniche [3], sezione 3, paragrafo 3.1:

> *Le attuali implementazioni di Shibboleth permettono all'amministratore di un IdP di scegliere, fra le altre, due modalità di base per presentare all'utente la richiesta di credenziali per l'autenticazione:*
> *• una soluzione (Apache-based) consiste nell'appoggiarsi direttamente sul server web: l'IdP presenta una finestra di pop-up (del browser) in cui l'utente inserisce le proprie credenziali;*
> *• la soluzione alternativa (Java-based) utilizza l'autenticazione attraverso JAAS (Java Authentication and Authorization Service): questa seconda modalità presenta all'utente il form di autenticazione inserito in una pagina web, che può essere personalizzata applicando gli stessi stili dell'organizzazione che amministra l'IdP.*
>
> *È evidente come la possibilità di modellare il form di autenticazione secondo lo stile del sito dell'organizzazione di apparteneza dell'utente aggiunga un tocco di family-feeling al processo di inserimento delle credenziali. L'utente sarebbe decisamente piu' disorientato nel veder comparire sul proprio browser un pop-up senza alcun tipo di spiegazione. La modalità Java-based aggiunge inoltre la possibilità di guidare l'utente nell'autenticazione, poichè permette di inserire nella pagina web istruzioni, riferimenti tecnici ecc..*
> *In conclusione, la Federazione consiglia fortemente l'utilizzo della modalità di autenticazione Javabased.*
> ***N.B. Nel caso di contesti in cui è utilizzato CAS valgono le stesse considerazioni fatte per JAAS.***

In definitiva, il documento nella formulazione **non stabilisce obblighi** nella composizione della pagina di login ma solo consigli

Problematiche Emergenti

L'adozione di obblighi imposti ai gestori degli IdP in merito alla composizione della pagina di login come sarebbe desiderabile comporterebbe:

1. L’eliminazione della possibilità di attuare una autenticazione basata su pop-up
2. L’obbligo di inserire nella pagina web contenente il form di login un set minimo di requisiti (**almeno** un riferimento alla federazione sotto forma di logo con link alla pagina di ‘presentazione’ o di ‘contatto tecnico’)

Il punto 1 non implica difficoltà tecniche nè organizzative. Shibboleth (l’unico software ufficialmente supportato dalla federazione) permette agevolmente l’autenticazione basata su pagina web, e dal punto di vista organizzativo tale metodo ha solo punti a proprio favore.
Il punto 2 è ampiamente attuabile nelle pagine di login dedicate unicamente al SSO IDEM, ed è tecnicamente attuabile per le pagine che consentono il login anche ad altri servizi, così come dimostra la pagina di login CAS dell’Università di Parma [4]. Nel caso di sistemi legacy di autenticazione centralizzata, si deve tenere conto del comfort dell’utente nella navigazione di una pagina nota: per questo motivo è ragionevole che il requisito minimo sia quello espresso nel punto 2, ma dove possibile la pagina web dovrebbe riportare una quantità maggiore di informazioni e riferimente alla Federazione IDEM (link al sito, mission, etc.)

Soluzione Proposta

Mutuando l’approccio della sezione “9.1 Pagina associata all'IdP”, la sezione 3 è stata riscritta (vedi qui sotto nuova bozza) formulando delle linee guida ‘obbligatorie’, che prevedono l’eliminazione del supporto all’autenticazione Apache Based (pop-up) e la obbligatorietà dell’approccio web based con form.
Viene poi introdotto l’obbligo per la pagina di login di contenere almeno un riferimento ad IDEM tramite un testo od un logo che diano accesso alla pagina ‘contatto tecnico’. Viene inoltre suggerito di fornire, all’interno della pagina di login, un contesto alla navigazione utente che indichi chiaramente che tale accesso avviene/può avvenire tramite autenticazione federata IDEM.

Bozza nuova sezione 3
3 Autenticazione
3.1 Login dell’utente

La pagina web da presentare all'utente con la richiesta di credenziali per l'autenticazione (pagina di Login) deve aderire a precise linee guida ovvero deve soddisfare i requisiti obbligatori sotto indicati. Tali requisiti saranno verificati al momento della richiesta di registrazione del servizio e periodicamente nell'ambito dell'attività di auditing (v. sezione Operatività del servizio).
In particolare tale pagina di Login deve obbligatoriamente:

a. *utilizzare l’autenticazione in modalità web based tramite form, ovvero utilizzando JAAS (Java Authentication and Authorization Service): questo metodo presenta all'utente il form di autenticazione inserito in una pagina web, che può essere personalizzata applicandovi le scelte stilistiche proprie dell'organizzazione che amministra l'IdP. E’ quindi espressamente vietato l’utilizzo della modalità di autenticazione basata su pop-up;*

b. *contenere ALMENO UN riferimento ipertestuale o logo di IDEM con link alla pagina di contatto tecnico;*

E’, inoltre, fortemente consigliato, ma non obbligatorio, inserire nella pagina di Login ulteriori informazioni che l'organizzazione ritenga utili a far conoscere e comprendere ai propri utenti quale sia l’utilizzo di IDEM per l’accesso ai servizi.
In particolare si consiglia di inserire nella pagina di Login:

- *un contesto alla navigazione utente che indichi chiaramente che l’ accesso al servizio avviene/può avvenire tramite sistema di autenticazione federata IDEM;*
- *informazioni relative alle credenziali di accesso ed a come ottenerle in base al proprio profilo utente;*
- *informazioni su IDEM e sulle modalità di adesione ad IDEM;*
- *in caso di pagine di autenticazione centralizzata legacy (tipo CAS), che diventa anche pagina di*

autenticazione per IDEM, il requisito b) può essere soddisfatto in modo 'discreto' in modo da non disturbare la familiarità sviluppata dagli utenti.

Conclusioni

La proposta viene presentata al CTS per approvazione

Riferimenti

1 - http://aai.caspur.it/GARR-AAI-fed/index.php/Riunione_CTS_II#ToDo
2 - https://bridge.si.unimib.it/cas_all_unimib/login
3 - https://www.idem.garr.it/index.php/it/documenti/doc_download/105-specifichetecnichev1120100305
4 - https://cas.unipr.it/login